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. 144-164

<http://www.numdam.org/item?id=BSMA_1877_2_1_1_144_1>

MÉLANGES.

SUR LA THÉORIE DES NOMBRES ENTIERS ALGÉBRIQUES (¹);

PAR R. DEDEKIND.

(Suite.)

III.

PROPRIÉTÉS GÉNÉRALES DES NOMBRES ALGÉBRIQUES ENTIERS.

Dans cette Section nous considérerons d'abord le domaine de tous les nombres algébriques entiers ; nous introduirons ensuite la notion du corps fini Ω, et nous déterminerons la constitution du domaine $\mathfrak{o}$, composé de tous les nombres entiers du corps Ω.

§ 13. — *Le domaine de tous les nombres algébriques entiers.*

Un nombre réel ou complexe θ sera dit un nombre *algébrique*, lorsqu'il satisfera à une équation

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

de degré fini n et à coefficients rationnels $a_1, a_2, \ldots, a_{n-1}, a_n$; si cette équation a pour coefficients des nombres *rationnels entiers*, c'est-à-dire des nombres de la suite $0, \pm 1, \pm 2, \ldots$, θ sera dit un nombre *algébrique entier*, ou simplement un nombre *entier*. Il

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

est clair que les nombres rationnels entiers appartiennent également aux nombres algébriques entiers, et que, réciproquement, si un nombre rationnel θ est en même temps un nombre algébrique entier, il sera aussi, en vertu d'un théorème connu, contenu dans le domaine des nombres rationnels entiers $0, \pm 1, \pm 2, \ldots$. De la définition des nombres entiers on tire encore aisément les propositions suivantes :

1° Les nombres entiers se reproduisent par addition, soustraction et multiplication, c'est-à-dire que les sommes, les différences et les produits de deux nombres entiers quelconques α, β sont aussi des nombres entiers.

Démonstration. — Par suite de l'hypothèse, il existe deux équations de la forme

$$\varphi(\alpha) = \alpha^a + p_1\alpha^{a-1} + \ldots + p_{a-1}\alpha + p_a = 0,$$
$$\psi(\beta) = \beta^b + q_1\beta^{b-1} + \ldots + q_{b-1}\beta + q_b = 0,$$

dans lesquelles tous les coefficients p, q sont des nombres rationnels entiers. Posons maintenant $ab = n$, et désignons par ω_1, $\omega_2, \ldots, \omega_n$ tous les n produits $\alpha^{a'}\beta^{b'}$, formés avec l'un des a nombres

$$1, \quad \alpha, \quad \alpha^2, \quad \ldots, \quad \alpha^{a-1},$$

et l'un des b nombres

$$1, \quad \beta, \quad \beta^2, \quad \ldots, \quad \beta^{b-1}.$$

En représentant maintenant par ω l'un des trois nombres $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, on voit facilement que chacun des n produits $\omega\omega_1$, $\omega\omega_2, \ldots, \omega\omega_n$ peut se ramener soit immédiatement, soit à l'aide des équations $\varphi(\alpha) = 0$, $\psi(\beta) = 0$, à la forme

$$k_1\omega_1 + k_2\omega_2 + \ldots + k_n\omega_n,$$

$k_1, k_2, \ldots, k_n$ étant des nombres rationnels *entiers;* on a donc n équations de la forme

$$\omega\omega_1 = k'_1\omega_1 + k'_2\omega_2 + \ldots + k'_n\omega_n,$$
$$\omega\omega_2 = k''_1\omega_1 + k''_2\omega_2 + \ldots + k''_n\omega_n,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$
$$\omega\omega_n = k_1^{(n)}\omega_1 + k_2^{(n)}\omega_2 + \ldots + k_n^{(n)}\omega_n,$$

tous les coefficients k étant des nombres rationnels entiers ; mais, par l'élimination des n nombres $\omega_1, \omega_2, \ldots, \omega_n$, parmi lesquels se trouve aussi le nombre 1, différent de zéro, on tire de là l'équation

$$\begin{vmatrix} k'_1 - \omega & k'_2 & \ldots & k'_n \\ k''_1 & k''_2 - \omega & \ldots & k''_n \\ \ldots & \ldots\ldots & \ldots & \ldots \\ k_1^{(n)} & k_2^{(n)} & \ldots & k_n^{(n)} - \omega \end{vmatrix} = 0,$$

qui est évidemment de la forme

$$\omega^n + e_1\omega^{n-1} + \ldots + e_{n-1}\omega + e_n = 0,$$

où les n coefficients e sont formés par addition, soustraction et multiplication au moyen des nombres k, et par suite sont des nombres rationnels entiers. Donc ω, et partant chacun des trois nombres $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$ est un nombre entier. C. Q. F. D.

2° Toute racine ω d'une équation de la forme

$$F(\omega) = \omega^m + \alpha\omega^{m-1} + \beta\omega^{m-2} + \ldots + \varepsilon = 0,$$

dont le coefficient du terme le plus élevé est l'unité, les autres coefficients $\alpha, \beta, \ldots, \varepsilon$ étant des nombres entiers, est pareillement un nombre entier.

Démonstration. — Par suite de l'hypothèse, les coefficients $\alpha, \beta, \ldots, \varepsilon$ sont racines d'équations

$$\begin{aligned} \varphi(\alpha) &= \alpha^a + p_1\alpha^{a-1} + \ldots + p_a = 0, \\ \psi(\beta) &= \beta^b + q_1\beta^{b-1} + \ldots + q_b = 0, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ \chi(\varepsilon) &= \varepsilon^e + s_1\varepsilon^{e-1} + \ldots + s_e = 0, \end{aligned}$$

où tous les coefficients $p, q, \ldots, s$ désignent des nombres rationnels entiers. En posant maintenant $n = mab\ldots e$, et désignant par $\omega_1, \omega_2, \ldots, \omega_n$ tous les n produits de la forme

$$\omega^{m'}\alpha^{a'}\beta^{b'}\ldots\varepsilon^{e'},$$

où les exposants rationnels entiers satisfont aux conditions

$$0 \leqq m' < m, \quad 0 \leqq a' < a, \quad 0 \leqq b' < b, \quad \ldots, \quad 0 \leqq e' < e,$$

il est facile de s'assurer que chacun des produits $\omega\omega_1, \omega\omega_2, \ldots, \omega\omega_n$ peut, soit immédiatement, soit à l'aide des équations $F(\omega) = 0$, $\varphi(\alpha) = 0, \psi(\beta) = 0, \ldots, \chi(\varepsilon) = 0$, se ramener à la forme

$$k_1\omega_1 + k_2\omega_2 + \ldots + k_n\omega_n,$$

$k_1, k_2, \ldots, k_n$ représentant des nombres rationnels entiers. Or il suit de là, comme dans la démonstration du théorème précédent, que ω est un nombre entier. C. Q. F. D.

Du dernier théorème il résulte, par exemple, que, si α désigne un nombre entier quelconque, et r, s des nombres rationnels entiers positifs, $\sqrt[s]{\alpha^r}$ sera aussi un nombre entier.

§ 14. — *La divisibilité des nombres entiers.*

Nous dirons qu'un nombre entier α est *divisible* par un nombre entier β, lorsqu'on aura $\alpha = \beta\gamma$, γ étant également un nombre entier. Nous exprimerons encore la même chose en disant que α est un multiple de β, ou que β divise α, ou que β est un facteur ou un diviseur de α. De cette définition et du théorème 1° du § 13 résultent, comme nous l'avons déjà fait voir dans l'*Introduction*, ces deux propositions élémentaires :

1° Si α, α' sont divisibles par μ, $\alpha + \alpha'$ et $\alpha - \alpha'$ seront aussi divisibles par μ ;

2° Si α' est divisible par α et α divisible par μ, α' sera aussi divisible par μ.

Mais il faut accorder une attention particulière aux *unités*, c'est-à-dire aux nombres entiers qui divisent *tous* les nombres entiers ; une unité ε devra ainsi diviser le nombre 1, et réciproquement il est évident que tout diviseur ε du nombre 1 est une unité, puisque tout nombre entier est divisible par l'unité 1, et par suite aussi (en vertu de la proposition 2° ci-dessus) divisible par ε. On voit en même temps que tout produit ou tout quotient de deux unités est lui-même une unité.

Si chacun des deux nombres entiers α et α', différents de zéro, est divisible par l'autre, on aura $\alpha' = \alpha\varepsilon$, ε étant une unité ; et réciproquement, si ε est une unité, chacun des deux nombres entiers α et $\alpha' = \alpha\varepsilon$ sera divisible par l'autre. Nous donnerons à deux

nombres de cette nature α, α' le nom d'*associés*, et il est clair que deux nombres quelconques associés avec un troisième sont associés entre eux. Dans toutes les questions qui se rapportent seulement à la divisibilité, tous les nombres associés se comportent comme un seul et même nombre; si, en effet, α est divisible par β, tout nombre associé avec α sera aussi divisible par tout nombre associé avec β.

Un examen plus approfondi ferait voir que deux nombres entiers, α, β, qui ne sont pas tous les deux nuls, ont un *plus grand* commun diviseur, qui peut se mettre sous la forme $\alpha\alpha' + \beta\beta'$, et α' et β' étant des nombres entiers. Mais ce théorème important n'est nullement facile à démontrer à l'aide des principes exposés jusqu'ici, tandis que plus tard (§ 30) on pourra le déduire très-simplement de la théorie des idéaux. Je terminerai donc ces considérations préliminaires sur le domaine de *tous* les nombres entiers, par cette remarque, qu'il n'existe dans ce domaine absolument aucun nombre possédant le caractère des *nombres premiers;* car, si α est un nombre entier quelconque différent de zéro, et qui ne soit non plus une unité, on pourra le décomposer d'une infinité de manières en facteurs qui seront des nombres entiers et qui en même temps ne seront pas des unités; ainsi, par exemple, on a $\alpha = \sqrt{\alpha}.\sqrt{\alpha}$, ou encore $\alpha = \beta_1\beta_2$, β_1 et β_2 étant les deux racines β de l'équation $\beta^2 - \beta + \alpha = 0$; or il résulte du théorème 2° du § 13 que $\sqrt{\alpha}$, β_1, β_2 sont des nombres entiers en même temps que α.

§ 15. — *Corps finis.*

La propriété d'être décomposables d'une infinité de manières, que nous venons de signaler et qui se présente dans le domaine comprenant tous les nombres entiers, disparaît de nouveau dès que l'on se borne à considérer les nombres entiers renfermés dans un *corps fini*. Il faut d'abord définir l'étendue et la nature d'un tel corps.

Tout nombre algébrique θ, que ce soit ou non un nombre entier, satisfait évidemment à une infinité d'équations différentes à coefficients rationnels, c'est-à-dire qu'il y a une infinité de fonctions en-

tières $F(t)$ d'une variable t qui s'évanouissent pour $t = \theta$, et dont les coefficients sont rationnels. Mais, parmi toutes ces fonctions $F(t)$, il doit nécessairement y en avoir une $f(t)$ dont le degré n soit *le plus petit possible*, et de la méthode connue de la division de ces sortes de fonctions il résulte immédiatement que chacune des fonctions $F(t)$ doit être divisible algébriquement par cette fonction $f(t)$, et que $f(t)$ ne peut être divisible par aucune fonction entière de degré moindre à coefficients rationnels. Pour cette raison, la fonction $f(t)$ et aussi l'équation $f(\theta) = 0$ seront appelées *irréductibles*, et il est clair, en même temps, que les n nombres $1, \theta^1, \theta^2, \ldots, \theta^{n-1}$ formeront un *système irréductible* (§ 4, 1°).

Considérons maintenant l'ensemble Ω de tous les nombres ω de la forme $\varphi(\theta)$, en désignant par

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

toute fonction entière quelconque de t à coefficients rationnels, entiers ou fractionnaires, $x_0, x_1, x_2, \ldots, x_{n-1}$, dont le degré est $< n$, et remarquons d'abord que tout nombre de cette espèce $\omega = \varphi(\theta)$, en vertu de l'irréductibilité de $f(t)$, ne peut se mettre sous cette forme que d'une seule manière. On fait voir ensuite aisément que ces nombres ω se reproduisent toujours par les *opérations rationnelles*, c'est-à-dire par addition, soustraction, multiplication et division. Pour les deux premières opérations, cela résulte évidemment de la forme commune $\varphi(\theta)$ de tous les nombres ω, et pour la multiplication il suffit de remarquer que tout nombre de la forme $\psi(\theta)$, $\psi(t)$ étant une fonction entière de degré *quelconque*, à coefficients rationnels, est également un nombre ω; car, si l'on divise $\psi(t)$ par $f(t)$, le reste de la division sera une fonction $\varphi(t)$ de l'espèce indiquée plus haut, et l'on aura en même temps $\psi(\theta) = \varphi(\theta)$. Pour traiter enfin le cas de la division, on n'a plus qu'à faire voir encore que, si $\omega = \varphi(\theta)$ est différent de zéro, sa valeur réciproque ω^{-1} appartient aussi au système Ω; or $\varphi(t)$ n'ayant aucun diviseur commun avec la fonction irréductible $f(t)$, la méthode par laquelle on chercherait le plus grand commun diviseur des fonctions $f(t)$, $\varphi(t)$ fournit, comme on sait, deux fonctions entières $f_1(t)$, $\varphi_1(t)$, à coefficients rationnels, qui satisfont à l'i-

dentité

$$f(t)f_1(t) + \varphi(t)\varphi_1(t) = 1,$$

d'où résulte, pour $t = \theta$, la vérité de l'énoncé précédent.

J'appellerai *corps* tout système A de nombres a (ne s'annulant pas tous), tel que les sommes, les différences, les produits et les quotients de deux quelconques de ces nombres a appartiennent au système A. L'exemple le plus simple d'un corps est celui du système de tous les nombres rationnels, et il est aisé de reconnaître que ce corps est contenu dans tout autre corps A; car, si l'on choisit à volonté un nombre a du corps A, différent de zéro, il faut, suivant la définition, que le quotient 1 des deux nombres a et a appartienne également au corps A, d'où résulte immédiatement la proposition énoncée, tous les nombres rationnels pouvant être engendrés au moyen du nombre 1 par des additions, des soustractions, des multiplications et des divisions répétées.

D'après ce que nous avons démontré plus haut relativement aux nombres $\omega = \varphi(\theta)$, notre système Ω formera donc aussi un corps; les nombres rationnels se tirent de $\varphi(\theta)$, en annulant tous les coefficients $x_1, x_2, \ldots, x_{n-1}$ qui suivent x_0. Un corps Ω qui est produit, de la manière indiquée, par une équation irréductible $f(\theta) = 0$ du degré n, nous l'appellerons un corps *fini* [1], et le nombre n sera dit son *degré*. Un tel corps Ω contient n nombres indépendants entre eux, par exemple, les nombres $1, \theta, \theta^2, \ldots, \theta^{n-1}$, tandis que $n+1$ nombres quelconques du corps formeront évidemment un système réductible (§ 4, 1°); cette propriété, jointe à la notion de corps, pourrait aussi servir de définition pour un corps Ω du $n^{\text{ième}}$ degré; je n'entrerai pas toutefois dans la démonstration de cette assertion.

Si l'on choisit maintenant arbitrairement n nombres

$$\omega_1 = \varphi_1(\theta), \quad \omega_2 = \varphi_2(\theta), \ldots, \quad \omega_n = \varphi_n(\theta)$$

---

[1] Si l'on entend par diviseur d'un corps A tout corps B dont tous les nombres sont contenus aussi dans A, un corps fini pourra être encore défini comme un corps qui ne possède qu'un nombre fini de diviseurs. En employant ici le mot *diviseur* (et le mot *multiple*) dans un sens directement opposé à celui que nous lui avons attaché, en parlant des modules et des idéaux, il ne pourra sûrement en résulter aucune confusion.

du corps Ω, ces nombres (d'après le § 4, 2°) formeront toujours, et seulement alors, un système irréductible, lorsque le déterminant formé avec les n^2 coefficients rationnels x sera différent de zéro; dans ce cas, nous appellerons le système des n nombres $\omega_1, \omega_2, \ldots, \omega_n$ une *base du corps* Ω; alors il est évident que tout nombre $\omega = \varphi(\theta)$ peut toujours, et d'une seule manière, se mettre sous la forme

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

les coefficients $h_1, h_2, \ldots, h_n$ étant des nombres rationnels, entiers ou fractionnaires, et réciproquement, tous les nombres ω de cette forme sont contenus dans Ω; les coefficients rationnels $h_1, h_2, \ldots, h_n$ seront dits les *coordonnées du nombre* ω par rapport à cette base.

§ 16. — *Corps conjugués.*

On entend ordinairement par *substitution* un acte par lequel les objets d'une étude ou les éléments d'une recherche sont remplacés par des objets ou des éléments correspondants, et l'on dit que les anciens éléments se changent, par la substitution, dans les nouveaux éléments. Soit maintenant Ω un corps *quelconque;* nous entendrons par une *permutation de* Ω une substitution par laquelle chaque nombre déterminé contenu dans Ω,

$$\alpha, \quad \beta, \quad \alpha+\beta, \quad \alpha-\beta, \quad \alpha\beta, \quad \frac{\alpha}{\beta},$$

se change dans un nombre déterminé correspondant

$$\alpha', \quad \beta', \quad (\alpha+\beta)', \quad (\alpha-\beta)', \quad (\alpha\beta)', \quad \left(\frac{\alpha}{\beta}\right)',$$

et cela de telle manière que les deux conditions

$$(1) \qquad (\alpha+\beta)' = \alpha'+\beta',$$

$$(2) \qquad (\alpha\beta)' = \alpha'\beta'$$

soient remplies, et que les nombres substitués $\alpha', \beta', \ldots$ ne s'annulent pas tous. Nous allons faire voir que l'ensemble Ω' de ces derniers nombres forme un nouveau *corps,* et que la permutation sa-

tisfait aussi aux deux conditions suivantes :

$$(3) \qquad (\alpha - \beta)' = \alpha' - \beta',$$

$$(4) \qquad \left(\frac{\alpha}{\beta}\right)' = \frac{\alpha'}{\beta'}.$$

Si l'on désigne, en effet, par α', β' deux nombres quelconques du système Ω', il existera dans le corps Ω deux nombres α, β, qui par la permutation se changeront respectivement en α', β'; or les nombres $\alpha + \beta$, $\alpha\beta$ étant également contenus dans Ω, il résulte de (1) et de (2) que les nombres $\alpha' + \beta'$, $\alpha'\beta'$ seront aussi contenus dans Ω'; donc les nombres du système Ω' se produisent par addition et multiplication. De plus, les nombres $\alpha = (\alpha - \beta) + \beta$ et $\alpha - \beta$ étant pareillement contenus dans Ω, il résulte de (1) que

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

ce qui constitue la condition (3); donc les nombres du système Ω' se reproduisent aussi par soustraction. Enfin, si β' est différent de zéro, alors, en vertu de (1), β sera aussi différent de zéro, et par suite $\frac{\alpha}{\beta}$ est un nombre déterminé appartenant au corps Ω; comme on a maintenant $\alpha = \left(\frac{\alpha}{\beta}\right)\beta$, il résulte de (2) que l'on a aussi $\alpha' = \left(\frac{\alpha}{\beta}\right)'\beta'$, ce qui constitue la condition (4); donc les nombres du système Ω' se reproduisent aussi par division, et par suite Ω' est un corps.

C. Q. F. D.

Remarquons maintenant, de plus, que, si $\beta' = 0$, on devra avoir aussi $\beta = 0$; car autrement *tout* nombre α du corps Ω pourrait se mettre sous la forme $\left(\frac{\alpha}{\beta}\right)\beta$, d'où résulterait $\alpha' = \left(\frac{\alpha}{\beta}\right)'\beta' = 0$, tandis que nous avons, au contraire, admis que les nombres α' du système Ω' ne s'annulent pas tous. Il suit de là évidemment, en ayant égard à (3), que, par une permutation, deux nombres *différents* α, β du corps Ω se changeront aussi en deux nombres *différents* α', β' du corps Ω', et qu'ainsi chaque nombre déterminé α' du corps Ω' ne correspond qu'à un seul nombre complétement déterminé α du corps Ω. La correspondance peut donc être renversée d'une manière univoque, et la substitution par laquelle chaque nombre déterminé α' du corps Ω' se changera dans le nombre cor-

respondant α du corps Ω sera une *permutation du corps* Ω', puisqu'elle satisfera aux conditions caractéristiques (1) et (2). Chacune de ces deux permutations sera dite l'*inverse* de l'autre; nous appellerons, de plus, Ω et Ω' des *corps conjugués*, et de même deux nombres correspondants quelconques α, α' des *nombres conjugués*. Il existe évidemment pour chaque corps Ω une permutation que nous nommerons la permutation *identique* de Ω, et qui consiste en ce que chaque nombre du corps Ω sera remplacé par lui-même; donc tout corps est conjugué à lui-même. En outre, il est facile de s'assurer que deux corps conjugués à un troisième sont aussi conjugués entre eux; car, si chaque nombre α du corps Ω se change, par une permutation P, en un nombre α' du corps Ω', et que pareillement chaque nombre α' de ce dernier se change, par une permutation P', en un nombre α'' du corps Ω'', il est clair que la substitution par laquelle chaque nombre α du corps Ω se change dans le nombre correspondant α'' du corps Ω'' est également une *permutation* du corps Ω, et nous la désignerons par PP'. Si l'on désigne par P^{-1} la permutation inverse de P, alors PP^{-1} sera la permutation identique de Ω, et Ω'' se changera en Ω par la permutation

$$(PP')^{-1} = P'^{-1} P^{-1}.$$

Nous avons déjà remarqué que chaque corps renferme tous les nombres rationnels, et il est aisé de montrer que chacun de ceux-ci, par une permutation du corps, se change toujours en lui-même; car, si l'on prend $\alpha = \beta$, il résulte de (4) que l'on aura $1' = 1$; or, tout nombre rationnel pouvant être engendré du nombre 1 par une série d'opérations rationnelles, notre proposition s'ensuit immédiatement des propriétés (1), (2), (3), (4). Soit de plus θ un nombre quelconque du corps Ω, et $R(t)$ une fonction rationnelle quelconque de la variable t à coefficients rationnels; le nombre $\omega = R(\theta)$, au cas où le dénominateur de la fonction $R(t)$ ne s'annule pas pour $t = 0$, sera aussi contenu dans Ω, et si, par une permutation du corps, θ se change dans le nombre θ', alors le nombre ω, étant formé par des opérations rationnelles exécutées sur le nombre θ et sur les coefficients rationnels de $R(t)$, se changera, par la même permutation, dans le nombre $\omega' = R(\theta')$. De là résulte immédiatement que, si θ est un nombre algébrique et satisfait, par suite, à une équation de la forme $0 = F(\theta)$ dont les coefficients soient

des nombres rationnels, on devra avoir aussi $o = F(\theta')$; donc tout nombre θ' conjugué à un nombre algébrique θ est également un nombre algébrique; et si θ est un nombre entier, θ' sera aussi un nombre entier.

Après ces considérations générales, qui sont relatives à *tous* les corps, revenons à notre exemple, où il s'agit d'un corps fini Ω, de degré n, et proposons-nous le problème de trouver *toutes* les permutations de Ω. Tous les nombres ω d'un tel corps Ω étant, d'après le § 15, de la forme $\varphi(\theta)$, θ désignant une racine d'une équation irréductible $o = f(\theta)$ du degré n, une permutation de Ω, en vertu de ce qui précède, sera déjà complétement déterminée par le choix de la racine θ' de l'équation $o = f(\theta')$, dans laquelle θ se change, puisqu'en même temps tout nombre $\omega = \varphi(\theta)$ devra se changer en $\omega' = \varphi(\theta')$. Réciproquement, si l'on choisit pour θ' une racine quelconque de l'équation $o = f(\theta')$, et que l'on remplace chaque nombre $\omega = \varphi(\theta)$ du corps Ω par le nombre correspondant $\omega' = \varphi(\theta')$, cette substitution sera réellement une permutation de Ω, c'est-à-dire qu'elle satisfera aux conditions (1) et (2). Pour le démontrer, désignons par $\varphi_1(t)$, $\varphi_2(t)$, ... des fonctions spéciales quelconques, de la forme $\varphi(t)$; si l'on a maintenant

$$\alpha = \varphi_1(\theta), \quad \beta = \varphi_2(\theta), \quad \alpha + \beta = \varphi_3(\theta), \quad \alpha\beta = \varphi_4(\theta),$$

et par suite

$$\alpha' = \varphi_1(\theta'), \quad \beta' = \varphi_2(\theta'), \quad (\alpha + \beta)' = \varphi_3(\theta'), \quad (\alpha\beta)' = \varphi_4(\theta'),$$

il résulte des équations

$$\varphi_3(\theta) = \varphi_1(\theta) + \varphi_2(\theta), \quad \varphi_4(\theta) = \varphi_1(\theta)\varphi_2(\theta),$$

et de l'irréductibilité de la fonction $f(t)$, que l'on aura identiquement

$$\varphi_3(t) = \varphi_1(t) + \varphi_2(t), \quad \varphi_4(t) = \varphi_1(t)\varphi_2(t) + \varphi_5(t)f(t),$$

ce qui donne, en faisant $t = \theta'$, les équations (1) et (2) qu'il s'agissait de démontrer. Si donc on pose

$$f(t) = (t - \theta')(t - \theta'')\ldots(t - \theta^{(n)}),$$

les n racines $\theta', \theta'', \ldots, \theta^{(n)}$ seront inégales, puisque la fonction

irréductible $f(t)$ ne peut avoir aucun diviseur commun avec sa dérivée $f'(t)$, et à chacune d'elles correspondra une permutation P', P'', ..., $P^{(n)}$ du corps Ω, de telle manière que, par la permutation $P^{(r)}$, chaque nombre $\omega = \varphi(\theta)$ du corps Ω se change dans le nombre conjugué $\omega^{(r)} = \varphi(\theta^{(r)})$ du corps conjugué $\Omega^{(r)}$. Pour éviter les malentendus, nous ferons observer que ces n corps conjugués $\Omega^{(r)}$, bien qu'ils se déduisent de Ω par n permutations *différentes*, peuvent très-bien être cependant identiques entre eux quant à l'ensemble des nombres qu'ils contiennent, soit en partie, soit en totalité; s'ils sont tous identiques, Ω sera dit un *corps de Galois* ou bien un *corps normal*. Les principes algébriques de Galois consistent en ce que l'étude des corps finis quelconques est ramenée à celle des corps normaux; mais le manque d'espace ne me permet pas maintenant de m'étendre davantage sur ce sujet.

§ 17. — *Normes et discriminants.*

Par la *norme* $N(\omega)$ d'un nombre quelconque ω du corps Ω de degré n nous entendrons le produit

$$N(\omega) = \omega'\omega'' \ldots \omega^{(n)} \tag{1}$$

des n nombres conjugués ω', ω'', ..., $\omega^{(n)}$, dans lesquels ω se change par les permutations P', P'', ..., $P^{(n)}$. Elle ne peut s'annuler que si l'on a $\omega = 0$. Si ω est un nombre rationnel, alors tous les n nombres $\omega^{(r)}$ seront égaux à ω, et par suite la norme d'un nombre rationnel est la $n^{\text{ième}}$ puissance de ce nombre. Si α, β sont deux nombres quelconques du corps Ω, on aura $(\alpha\beta)^{(r)} = \alpha^{(r)}\beta^{(r)}$, et par conséquent

$$N(\alpha\beta) = N(\alpha)N(\beta). \tag{2}$$

Par le *discriminant* $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$ d'un système quelconque de n nombres $\alpha_1, \alpha_2, \ldots, \alpha_n$ du corps Ω, nous entendrons le carré

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\Sigma \pm \alpha'_1 \alpha''_2 \ldots \alpha_n^{(n)})^2 \tag{3}$$

du déterminant formé avec les n^2 nombres $\alpha_i^{(r)}$. De là résulte, en vertu d'une proposition bien connue de la théorie des détermi-

nants, la relation

$$\Delta(1, \theta, \theta^2, \ldots, \theta^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} \mathrm{N}[f'(\theta)], \tag{4}$$

et comme $f'(\theta)$ ne peut pas, à cause de l'irréductibilité de la fonction $f(t)$, devenir égale à zéro, il s'ensuit que le discriminant (4) a une valeur différente de zéro.

Si maintenant les n nombres $\omega_1, \omega_2, \ldots, \omega_n$ forment une *base* du corps Ω (§ 15), et que

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

soit un nombre quelconque de ce corps, alors, puisque ses coordonnées $h_1, h_2, \ldots, h_n$ sont des nombres rationnels, la permutation $\mathrm{P}^{(r)}$ changera ω dans le nombre

$$\omega^{(r)} = h_1\omega_1^{(r)} + h_2\omega_2^{(r)} + \ldots + h_n\omega_n^{(r)},$$

et l'on tire de là

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = a^2\Delta(\omega_1, \omega_2, \ldots, \omega_n), \tag{5}$$

a désignant le déterminant formé avec les n^2 coordonnées des n nombres $\alpha_1, \alpha_2, \ldots, \alpha_n$. On en conclut d'abord que le discriminant de la base $\omega_1, \omega_2, \ldots, \omega_n$ ne peut s'évanouir, parce que, autrement, *tout* discriminant devrait s'évanouir, tandis que, au contraire, on a fait voir plus haut que $\Delta(1, \theta, \ldots, \theta^{n-1})$ est différent de zéro. Il s'ensuit en même temps que $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$ s'annule toujours, et seulement alors quand les nombres $\alpha_1, \alpha_2, \ldots, \alpha_n$ sont dépendants les uns des autres (§ 4, 2°), et par suite ne forment pas une base de Ω.

Puisque les nombres du corps se reproduisent par multiplication, on pourra poser, μ étant un nombre quelconque compris dans Ω,

$$\left\{\begin{aligned} \mu\omega_1 &= m_{1,1}\omega_1 + m_{2,1}\omega_2 + \ldots + m_{n,1}\omega_n, \\ \mu\omega_2 &= m_{1,2}\omega_1 + m_{2,2}\omega_2 + \ldots + m_{n,2}\omega_n, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ \mu\omega_n &= m_{1,n}\omega_1 + m_{2,n}\omega_2 + \ldots + m_{n,n}\omega_n, \end{aligned}\right. \tag{6}$$

où les n^2 coordonnées $m_{i,i'}$ sont des nombres rationnels; de là ré-

sultent, par les n permutations $P^{(r)}$, n^2 nouveaux nombres de la forme

$$\mu^{(r)}\omega_i^{(r)} = m_{1,i}\omega_1^{(r)} + m_{2,i}\omega_2^{(r)} + \ldots + m_{n,i}\omega_n^{(r)},$$

et, comme leur déterminant est

$$N(\mu)\Sigma\pm\omega'_1\omega''_2\ldots\omega_n^{(n)} = \Sigma\pm m_{1,1}m_{2,2}\ldots m_{n,n}\cdot\Sigma\pm\omega'_1\omega''_2\ldots\omega_n^{(n)},$$

on en conclut

$$N(\mu) = \Sigma\pm m_{1,1}m_{2,2}\ldots m_{n,n}, \tag{7}$$

puisque le déterminant

$$\Sigma\pm\omega'_1\omega''_2\ldots\omega_n^{(n)} = \sqrt{\Delta(\omega_1, \omega_2, \ldots, \omega_n)}$$

n'est pas nul.

Il suit de là que toute norme est un nombre *rationnel*, et la même conséquence, en vertu de (4) et (5), s'applique aussi à tout discriminant; ces deux propositions auraient pu aussi se déduire de la théorie de la transformation des fonctions symétriques, dont j'ai, à dessein, évité ici de me servir.

Si l'on remplace, dans les équations (6), le nombre μ par $\mu - z$, z étant un nombre rationnel quelconque, les coordonnées $m_{i,i'}$ n'éprouveront aucun changement, à l'exception des coordonnées $m_{i,i}$, qui se trouvent sur la diagonale, et qui devront être remplacées par $m_{i,i} - z$. Le théorème (7) se trouve ainsi changé dans l'égalité

$$\begin{vmatrix} m_{1,1}-z & m_{2,1} & \ldots & m_{n,1} \\ m_{1,2} & m_{2,2}-z & \ldots & m_{n,2} \\ \ldots & \ldots\ldots & \ldots & \ldots \\ m_{1,n} & m_{2,n} & \ldots & m_{n,n}-z \end{vmatrix} = (\mu'-z)(\mu''-z)\ldots(\mu^{(n)}-z),$$

laquelle, ayant lieu pour *toute* valeur rationnelle de z, devra nécessairement être une *identité* relativement à z. On voit en même temps que les n nombres $\mu', \mu'', \ldots, \mu^{(n)}$, conjugués à un nombre μ, forment l'ensemble des racines d'une équation du $n^{\text{ième}}$ degré, dont les coefficients sont des nombres rationnels.

§ 18. — *Le domaine* o *de tous les nombres entiers d'un corps fini* Ω.

Après ces préliminaires, nous allons passer à l'objet même que nous avons en vue, savoir, la considération de tous les nombres *entiers* contenus dans le corps Ω du degré n, nombres dont nous désignerons l'ensemble par o. Puisque les sommes, les différences et les produits de deux nombres entiers quelconques (d'après le § 13, 1°) sont encore des nombres entiers et (en vertu du § 15) sont aussi compris dans Ω, les nombres du domaine o, parmi lesquels se trouvent aussi tous les nombres *rationnels* entiers, se reproduiront aussi par addition, soustraction et multiplication. Mais il s'agit avant tout de mettre tous ces nombres sous une forme commune et simple. On y est conduit par les considérations suivantes :

Tout nombre algébrique ω étant racine d'une équation de la forme

$$c\omega^m + c_1\omega^{m-1} + \ldots + c_{m-1}\omega + c_m = 0,$$

dont les coefficients c, c_1, ..., c_{m-1}, c_m sont des nombres rationnels entiers, il en résulte, en multipliant par c^{m-1}, que tout nombre ω de cette espèce au moyen de la multiplication par un nombre rationnel entier c, différent de zéro, peut être changé en un nombre entier $c\omega$. Si maintenant les n nombres $\omega_1, \omega_2, \ldots, \omega_n$ forment une base du corps Ω, on pourra prendre les nombres rationnels $a_1, a_2, \ldots, a_n$, différents de zéro, de telle manière que les n nombres

$$\alpha_1 = a_1\omega_1, \quad \alpha_2 = a_2\omega_2, \quad \ldots, \quad \alpha_n = a_n\omega_n$$

deviennent des nombres *entiers*, et ceux-ci évidemment formeront encore une base du corps Ω, puisqu'ils sont (en vertu du § 4, 2°) indépendants les uns des autres. Par conséquent (d'après le § 17), leur discriminant $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$ sera un nombre rationnel, et même *entier*, différent de zéro, puisque, suivant sa définition, il est formé par addition, soustraction et multiplication de nombres tous entiers $\alpha_i^{(r)}$. On obtient, de plus, tous les nombres ω du corps Ω, en faisant prendre, dans l'expression

$$\omega = x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n,$$

aux coefficients $x_1, x_2, \ldots, x_n$ toutes les valeurs rationnelles; si on ne leur attribue que des valeurs rationnelles *entières,* on est certain alors de n'obtenir que des nombres *entiers* ω (§ 13, 1°); mais il est très-possible que l'on ne puisse pas représenter de cette manière *tous* les nombres entiers du corps Ω. A ce cas se rapporte ce théorème très-important :

S'il existe un nombre entier β *de la forme*

$$\beta = \frac{k_1\alpha_1 + k_2\alpha_2 + \ldots + k_n\alpha_n}{k},$$

$k, k_1, k_2, \ldots, k_n$ *étant des nombres rationnels entiers sans diviseur commun, il existera une base du corps* Ω, *formée de n nombres entiers* $\beta_1, \beta_2, \ldots, \beta_n$, *qui satisfera à la condition*

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = k^n \Delta(\beta_1, \beta_2, \ldots, \beta_n).$$

Démonstration. — Puisque $\beta, \alpha_1, \alpha_2, \ldots, \alpha_n$ sont des nombres entiers, ils formeront la base d'un module $\mathfrak{b} = [\beta, \alpha_1, \alpha_2, \ldots, \alpha_n]$, ne contenant que des nombres entiers du corps Ω; mais comme, de ces $n+1$ nombres, n seulement sont indépendants entre eux, il existera (§ 4, 5°) n nombres indépendants $\beta_1, \beta_2, \ldots, \beta_n$, qui formeront une base du même module $\mathfrak{b} = [\beta_1, \beta_2, \ldots, \beta_n]$, et qui seront, par suite, des nombres entiers du corps. On aura donc $n+1$ égalités de la forme

$$\begin{aligned}
\beta &= c_1\beta_1 + c_2\beta_2 + \ldots + c_n\beta_n,\\
\alpha_1 &= c_{1,1}\beta_1 + c_{2,1}\beta_2 + \ldots + c_{n,1}\beta_n,\\
\alpha_2 &= c_{1,2}\beta_1 + c_{2,2}\beta_2 + \ldots + c_{n,2}\beta_n,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
\alpha_n &= c_{1,n}\beta_1 + c_{2,n}\beta_2 + \ldots + c_{n,n}\beta_n,
\end{aligned}$$

dont tous les $n(n+1)$ coefficients seront des nombres rationnels entiers, et en même temps seront tels que les $n+1$ déterminants partiels du $n^{\text{ième}}$ degré que l'on peut former par la suppression d'une ligne horizontale quelconque n'auront *aucun* diviseur commun (§ 4, 6°). Si l'on pose

$$\Sigma \pm c_{1,1}c_{2,2}\ldots c_{n,n} = c,$$

on aura [§ 17 (5)]

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = c^2 \Delta(\beta_1, \beta_2, \ldots, \beta_n).$$

Or, en substituant les expressions précédentes de $\beta, \alpha_1, \alpha_2, \ldots, \alpha_n$ dans l'équation $k\beta = k_1\alpha_1 + k_2\alpha_2 + \ldots + k_n\alpha_n$, et observant que $\beta_1, \beta_2, \ldots, \beta_n$ sont indépendants entre eux, il en résulte

$$\begin{aligned} kc_1 &= k_1 c_{1,1} + k_2 c_{1,2} + \ldots + k_n c_{1,n}, \\ kc_2 &= k_1 c_{2,1} + k_2 c_{2,2} + \ldots + k_n c_{2,n}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ kc_n &= k_1 c_{n,1} + k_2 c_{n,2} + \ldots + k_n c_{n,n}; \end{aligned}$$

si l'on remplace maintenant les éléments

$$c_{1,r}, \quad c_{2,r}, \quad \ldots, \quad c_{n,r}$$

de la $r^{\text{ième}}$ ligne horizontale du déterminant c respectivement par les éléments

$$c_1, \quad c_2, \quad \ldots, \quad c_n,$$

on conclura des équations précédentes, en vertu d'un théorème connu, que le déterminant partiel ainsi obtenu a pour valeur $\frac{ck_r}{k}$. Donc les $n + 1$ quantités

$$\frac{ck}{k}, \quad \frac{ck_1}{k}, \quad \frac{ck_2}{k}, \quad \ldots, \quad \frac{ck_n}{k}$$

sont des nombres rationnels entiers sans diviseur commun, et comme il en est de même des $n + 1$ nombres $k, k_1, k_2, \ldots, k_n$, il faut donc que l'on ait $c = \pm k$. C. Q. F. D.

Si l'on a $k > 1$, et qu'ainsi le nombre entier β ne soit pas contenu dans le module $\mathfrak{a} = [\alpha_1, \alpha_2, \ldots, \alpha_n]$, il existera donc une base du corps, composée de n nombres entiers $\beta_1, \beta_2, \ldots, \beta_n$, dont le discriminant $\Delta(\beta_1, \beta_2, \ldots, \beta_n)$, pris en valeur absolue, sera $< \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Or, puisque, comme on l'a montré plus haut, le discriminant de toute base du corps Ω composée de nombres entiers est un nombre rationnel entier différent de zéro, il devra exister aussi une telle base $\omega_1, \omega_2, \ldots, \omega_n$, dont le discriminant

$$\Delta(\omega_1, \omega_2, \ldots, \omega_n) = \mathrm{D},$$

pris en valeur absolue, aura la valeur *minimum*, et de ce qui précède, il s'ensuit immédiatement que, relativement à une telle base, tout nombre entier

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

du corps Ω devra nécessairement avoir pour coordonnées des nombres *entiers* $h_1, h_2, \ldots, h_n$, et qu'un nombre entier ω n'est divisible par un nombre rationnel entier k que si toutes ses coordonnées sont divisibles par k. Comme, réciproquement, tout système de coordonnées entières $h_1, h_2, \ldots, h_n$ produit toujours un nombre entier ω, *l'ensemble* $\mathfrak{o}$ *de tous les nombres entiers du corps* Ω *est identique avec le module fini* $[\omega_1, \omega_2, \ldots, \omega_n]$ dont la base se compose des n nombres entiers indépendants $\omega_1, \omega_2, \ldots, \omega_n$.

Le discriminant D d'une telle base est un invariant du corps Ω, d'une importance fondamentale; nous l'appellerons pour cette raison le *nombre fondamental* ou le *discriminant du corps* Ω, et nous le représenterons par $\Delta(\Omega)$. Dans le cas singulier de $n = 1$, Ω est le corps des nombres *rationnels*, et par son discriminant nous entendrons le nombre $+1$. Comme éclaircissement, nous allons encore considérer le cas de $n = 2$, c'est-à-dire le cas d'un *corps quadratique*.

Toute racine θ d'une équation quadratique irréductible est de la forme

$$\theta = a + b\sqrt{d},$$

d étant un nombre rationnel entier complétement déterminé, qui n'est pas un carré, et qui, de plus, n'est divisible par aucun carré (excepté 1); a, b sont des nombres rationnels, et b est différent de zéro. L'ensemble de tous les nombres $\varphi(\theta)$ du corps quadratique correspondant Ω est évidemment identique avec l'ensemble de tous les nombres de la forme

$$\omega = t + u\sqrt{d},$$

où t, u prennent toutes les valeurs rationnelles. Par la permutation non identique du corps, $\sqrt{d}$ se change en $-\sqrt{d}$, et par suite ω dans le nombre conjugué

$$\omega' = t - u\sqrt{d},$$

lequel est également contenu dans Ω; donc Ω est un corps normal (§ 16). Pour rechercher tous les nombres *entiers* ω, posons

$$t = \frac{x}{z}, \quad u = \frac{y}{z},$$

x, y, z étant des nombres rationnels entiers sans diviseur commun, dont le dernier, z, peut être supposé positif. Si maintenant ω est un nombre entier, ω' en sera aussi un (§ 16), et par suite

$$\omega + \omega' = \frac{2x}{z}, \quad \omega\omega' = \frac{x^2 - dy^2}{z^2}$$

devront être aussi des nombres entiers; et réciproquement, s'il en est ainsi, ω sera évidemment un nombre entier (§ 13). Soit actuellement e le plus grand commun diviseur de z et de x; il faudra que e^2 divise $x^2 - dy^2$, et par suite aussi dy^2 et enfin y^2, puisque d n'est divisible par aucun carré autre que 1; donc e devra aussi diviser y, et par conséquent être $= 1$, puisque z, x, y n'ont aucun diviseur commun. Puisque ainsi z est premier avec x et divise cependant $2x$, il faudra que l'on ait soit $z = 1$, soit $z = 2$. Dans le premier cas, $\omega = x + y\sqrt{d}$ est certainement un nombre entier; dans le second cas, x est impair, partant $x^2 \equiv 1 \pmod 4$, et comme on doit avoir $x^2 \equiv dy^2 \pmod 4$, il faut que y soit aussi impair, et que l'on ait par conséquent $d \equiv 1 \pmod 4$. Si donc cette condition n'est pas remplie, c'est-à-dire si l'on a $d \equiv 2$ ou $d \equiv 3 \pmod 4$, z devra être $= 1$, et par suite on aura $\mathfrak{o} = [1, \sqrt{d}]$, et

$$\mathrm{D} = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = 4d.$$

Mais si l'on a $d \equiv 1 \pmod 4$, z pourra aussi devenir $= 2$ [1] et l'on aura

$$\mathfrak{o} = \left[1, \frac{1+\sqrt{d}}{2}\right], \quad \text{et} \quad \mathrm{D} = \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = d.$$

---

[1] De là résulte, par exemple, pour le cas de $d = -3$, que les nombres entiers du corps ne sont pas *tous* contenus dans la forme $x + y\sqrt{-3}$, où x, y prennent toutes les valeurs rationnelles.

Ces deux cas peuvent aussi se réunir en un seul, en remarquant que l'on a, dans les deux, $\mathfrak{o} = \left[1, \frac{D+\sqrt{D}}{2}\right]$. Il est clair en même temps qu'un corps *quadratique* est déjà complétement déterminé par son discriminant D. Il n'en est plus ainsi pour le cas qui suit immédiatement, savoir pour le cas de $n = 3$, dans lequel, outre le discriminant, il se présente encore d'autres invariants, qui sont nécessaires pour la détermination complète d'un corps *cubique;* toutefois on ne pourra donner d'explication générale de ce fait qu'à l'aide de la théorie des *idéaux*.

Revenons à la considération d'un corps quelconque Ω du degré n, et ajoutons encore les remarques suivantes sur la divisibilité et la congruence des nombres dans le domaine $\mathfrak{o}$. Soient λ, μ deux de ces nombres, et supposons que λ soit divisible par μ; on aura, d'après la définition générale de la divisibilité (§ 14), $\lambda = \mu\omega$, ω étant un nombre entier, et comme, en vertu de la définition d'un corps, le quotient ω des deux nombres λ, μ appartient au corps Ω, ω sera également un nombre du domaine $\mathfrak{o}$. Le système $\mathfrak{m}$ de tous les nombres du corps Ω divisibles par μ se compose donc de tous les nombres de la forme $\mu\omega$, ω parcourant tous les nombres du domaine $\mathfrak{o} = [\omega_1, \omega_2, \ldots, \omega_n]$, c'est-à-dire tous les nombres de la forme

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

dont les coordonnées $h_1, h_2, \ldots, h_n$ sont des nombres rationnels entiers; on a par conséquent $\mathfrak{m} = [\mu\omega_1, \mu\omega_2, \ldots, \mu\omega_n]$. Nous dirons maintenant que deux nombres entiers α, β du domaine $\mathfrak{o}$ sont *congrus* par rapport au *module* μ, et nous poserons

$$\alpha \equiv \beta \pmod{\mu},$$

quand la différence $\alpha - \beta$ sera divisible par μ, et sera ainsi contenue dans $\mathfrak{m}$; par suite, cette congruence est tout à fait équivalente à la suivante :

$$\alpha \equiv \beta \pmod{\mathfrak{m}},$$

dont le sens a été expliqué au § 2; dans le cas contraire, α, β sont dits *incongrus* par rapport à μ. Si l'on entend par une *classe* par rapport au module μ l'ensemble de tous ceux des nombres contenus dans $\mathfrak{o}$ qui sont congrus à un nombre déterminé et par suite aussi

congrus entre eux suivant μ, alors, d'après la notation introduite au § 2, le nombre de ces classes différentes sera $= (\mathfrak{o}, \mathfrak{m})$, et comme les nombres entiers $\mu\omega_1, \mu\omega_2, \ldots, \mu\omega_n$, qui forment la base de $\mathfrak{m}$, sont liés aux nombres $\omega_1, \omega_2, \ldots, \omega_n$ par n équations de la forme (6), (§ 17), dans lesquelles les coefficients $m_{i,i'}$ sont nécessairement des nombres rationnels *entiers*, il résulte de l'équation suivante (7), jointe au théorème 4° du § 4, que ce nombre des classes est

$$(\mathfrak{o}, \mathfrak{m}) = \pm \mathrm{N}(\mu).$$

Le système $\mathfrak{m}$ est identique avec $\mathfrak{o}$ toujours, et seulement alors quand μ est une unité, et l'on a en même temps $\pm \mathrm{N}(\mu) = (\mathfrak{o}, \mathfrak{o}) = 1$.

Maintenant, tandis que, dans cette conception de la congruence, où un nombre déterminé μ n'entre que comme diviseur ou module, il règne une complète analogie avec la théorie des nombres rationnels, il se manifeste, comme nous l'avons déjà indiqué en détail dans l'Introduction et dans la Section II, des phénomènes tout nouveaux à propos de la question de la composition des nombres du domaine $\mathfrak{o}$ au moyen de facteurs appartenant à ce même domaine $\mathfrak{o}$. Ces phénomènes seront ramenés à des lois déterminées et simples par la *Théorie des idéaux*, dont nous traiterons les éléments dans la Section suivante.

(*A suivre.*)