MÉMORIAL DES SCIENCES MATHÉMATIQUES

O. ORE

Les corps algébriques et la théorie des idéaux

Mémorial des sciences mathématiques, fascicule 64 (1934)

<http://www.numdam.org/item?id=MSM_1934__64__1_0>

MÉMORIAL
DES
SCIENCES MATHÉMATIQUES

PUBLIÉ SOUS LE PATRONAGE DE

L'ACADÉMIE DES SCIENCES DE PARIS,

DES ACADÉMIES DE BELGRADE, BRUXELLES, BUCAREST, COÏMBRE, CRACOVIE, KIEW, MADRID, PRAGUE, ROME, STOCKHOLM (FONDATION MITTAG-LEFFLER), DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE, AVEC LA COLLABORATION DE NOMBREUX SAVANTS.

DIRECTEUR :

Henri VILLAT
Membre de l'Institut,
Professeur à la Sorbonne,
Directeur du « Journal de Mathématiques pures et appliquées ».

FASCICULE LXIV

Les corps algébriques et la théorie des idéaux

Par M. O. ORE

PARIS
GAUTHIER-VILLARS, ÉDITEUR
LIBRAIRE DU BUREAU DES LONGITUDES, DE L'ÉCOLE POLYTECHNIQUE
Quai des Grands-Augustins, 55.

1934

LES CORPS ALGÉBRIQUES

ET

LA THÉORIE DES IDÉAUX

Par M. O. ORE.

INTRODUCTION.

La théorie des nombres algébriques a été développée depuis les travaux classiques de Gauss, Dirichlet, Kummer, Dedekind, Kronecker, à un des plus complexes des domaines mathématiques. Je me suis donc limité dans cette exposition aux parties centrales de la théorie sans entrer dans l'étude des corps spéciaux. On y trouvera premièrement un discussion des propriétés fondamentales des nombres et corps algébriques, les normes, éléments primitifs, bases minimales et discriminants. Je n'ai pas abordé les problèmes voisins de la théorie des corps abstraits, l'approximation et les critères pour des nombres algébriques ont été traités brièvement.

Dans la représentation de la théorie des idéaux et la divisibilité des entiers algébriques, j'ai suivi principalement les idées de Dedekind. Pour le théorème fondamental je donne une démonstration fondée sur les idées nouvelles de Krull et de v. d. Waerden. J'ai traité ici particulièrement la théorie arithmétique des idéaux, les classes résiduaires pour des modules idéaux et les groupes additifs et multiplicatifs correspondants; les résultats de Wiman sur les racines primitives y sont inclus. J'espère traiter une autre fois la partie plus algébrique de la théorie des idéaux et la connexion entre les idéaux et les propriétés des équations algébriques. Le dernier Chapitre a été consacré à la théorie des unités et l'on y trouvera une démonstration simplifiée nouvelle du théorème de Dirichlet.

CHAPITRE I.

1. Nombres algébriques. Propriétés fondamentales. — Un nombre $\mathfrak{I}$ (réel ou complexe) est dit *nombre algébrique* s'il satisfait à une équation algébrique

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n = 0 \tag{1}$$

avec coefficients rationnels. On dit que $\mathfrak{I}$ est un *nombre algébrique entier* (ou simplement un *nombre entier*) s'il satisfait à une équation (1) avec des coefficients entiers. L'existence des nombres algébriques est immédiatement assurée par le théorème fondamental de l'algèbre.

On peut aussi, comme on le fait dans la théorie des corps abstraits, considérer le nombre algébrique $\mathfrak{I}$ seulement comme un *symbole* ayant la qualité que l'expression

$$\mathfrak{I}^n + a_1 \mathfrak{I}^{n-1} + \ldots + a_n$$

peut toujours être remplacée par zéro. Ce point de vue a l'avantage de rendre l'existence de cette grandeur évidente sans application du théorème fondamental. Dans la suite on peut adopter le premier point de vue.

Tout nombre de la forme $a + ib$ (a, b rationnels) est un nombre algébrique, ainsi de même a^n (n, a rationnels); toute expression composée rationnellement par des radicaux de nombres rationnels est un nombre algébrique, mais il n'y a qu'une classe spéciale des nombres algébriques exprimable dans cette forme, les équations (1) n'étant pas en général solubles par radicaux.

Il est superflu de s'arrêter davantage à des exemples spéciaux; il faut pourtant observer que tout nombre rationnel a est aussi un nombre algébrique et que a est un entier algébrique seulement dans le cas où a est un entier ordinaire. Soit en effet

$$a = \frac{p}{q}, \qquad (p, q) = 1, \tag{1}$$

alors une équation

$$a^n + a_1 a^{n-1} + \ldots + a_n = 0$$

à coefficients entiers est impossible parce qu'on en déduit

$$p^n = -q\,(a_1 p^{n-1} + \ldots + a_n q^{n-1}),$$

c'est-à-dire $(p, q) > 1$.

On voit aussi que chaque nombre algébrique non entier peut être représenté dans la forme

$$\mathfrak{I} = \frac{\Theta}{m},$$

où Θ est un nombre algébrique entier, et m un entier rationnel. Si l'on construit l'équation satisfaite par $m\mathfrak{I}$, le coefficient général sera $b_i = a_i m^i$ et il suffit donc, pour rendre $m\mathfrak{I}$ entier, de prendre pour m le plus petit dénominateur commun des a_i.

Tout nombre algébrique $\mathfrak{I}$ satisfait à une infinité d'équations de la forme (1), mais on déduit sans difficulté l'existence d'une équation unique (1), pour laquelle le degré n est un minimum. Cette équation s'appelle *équation caractéristique* de $\mathfrak{I}$, et le polynome correspondant $f(x)$ est complètement caractérisé par la propriété que ce polynome est irréductible, c'est-à-dire qu'il n'existe pas de décomposition $f(x) = g(x)\,h(x)$ sauf dans le cas trivial où l'un des polynomes (1) $g(x)$ et $h(x)$ est une constante.

Le *degré* du nombre algébrique $\mathfrak{I}$ est le degré du polynome caractéristique. Si $F(x) = 0$ est une équation arbitraire satisfaite par $\mathfrak{I}$, le polynome $F(x)$ est divisible par $f(x)$.

Un nombre algébrique entier peut aussi satisfaire à des équations à coefficients non entiers; par exemple, l'entier $\sqrt{2}$ est une racine de

$$x^3 - \frac{1}{2}x^2 - 2x + 1 = 0.$$

Mais il est d'importance de noter que l'équation caractéristique d'un nombre entier a toujours des coefficients entiers; cette observation est une conséquence directe du théorème de Gauss : *si le produit* $F(x) = F_1(x)\,F_2(x)$ *de deux polynomes a des coefficients entiers, chacun des facteurs l'aura aussi.*

Soient enfin

$$\mathfrak{I} = \mathfrak{I}_1, \mathfrak{I}_2, \ldots, \mathfrak{I}_n \tag{2}$$

les n racines de l'équation caractéristique de $\mathfrak{I}$, et posons

$$f(x) = (x - \mathfrak{I}_1)\ldots(x - \mathfrak{I}_n). \tag{3}$$

(1) Il s'agit dans la suite seulement des polynomes à coefficients rationnels.

On appelle les racines (2) les *nombres conjugués* de $\mathfrak{I}$; les nombres conjugués sont tous en même temps entiers ou non entiers. On dit parfois, qu'un nombre $\mathfrak{I}$ est *totalement réel*, si tous les nombres conjugués sont aussi réels, et aussi qu'un nombre algébrique est *totalement positif*, si tous les conjugués *réels* de $\mathfrak{I}$ sont positifs.

2. Approximation des nombres algébriques par nombres rationnels. — Un nombre *transcendant* est un nombre complexe non algébrique. Avant de considérer les propriétés spéciales des nombres algébriques, je vais faire quelques observations sur les relations entre les nombres algébriques et les nombres transcendants.

On doit à Cantor le théorème suivant :

L'ensemble des nombres algébriques est dénombrable. Ce théorème peut être déduit simplement du fait que l'ensemble de tous les polynomes a coefficients rationnels est dénombrable. L'ensemble de tous les nombres transcendants a par conséquent la puissance du continu.

Une démonstration constructive de l'existence des nombres transcendants a été donnée par Liouville le premier en appliquant une propriété générale importante des nombres algébriques. Soit $\mathfrak{I}$ un nombre algébrique réel de degré $n > 1$, et $\frac{p}{q}$, $(p, q) = 1$, une fraction rationnelle, considérée comme une valeur approximative de $\mathfrak{I}$. Alors on a

$$\left|\mathfrak{I} - \frac{p}{q}\right| \geqq \frac{M}{q^n}, \qquad q > 0 \tag{4}$$

où M est une constante positive qui ne dépend pas de q. Cette inégalité montre, que la bonté de l'approximation d'un nombre algébrique par des nombres rationnels est toujours limitée. La démonstration de (4) est très simple. Soit $f(x) = 0$ l'équation caractéristique de $\mathfrak{I}$; alors on a

$$\left|f(\mathfrak{I}) - f\left(\frac{p}{q}\right)\right| = \left|f\left(\frac{p}{q}\right)\right| = \frac{|N|}{q^n} \geqq \frac{1}{q^n}, \tag{5}$$

où N est un nombre entier ordinaire. A l'autre côté on obtient par la formule de la moyenne

$$\left|f(\mathfrak{I}) - f\left(\frac{p}{q}\right)\right| = \left|\mathfrak{I} - \frac{p}{q}\right| |f'(\xi)| \leqq \left|\mathfrak{I} - \frac{p}{q}\right| K, \tag{6}$$

où K est une borne supérieure de $f'(x)$ dans un intervalle fini contenant $\mathfrak{I}$; de (5) et (6) on déduit l'inégalité (4) de Liouville. D'après cette inégalité le nombre $\alpha = 1 + \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \ldots$ est nécessairement transcendant, l'approximation à α par des nombres rationnels étant trop bonne. Par la méthode de Liouville on peut déterminer des classes très étendues de nombres transcendants (Maillet, *voir* aussi Ore [1]).

Le résultat (4) presque trivial de Liouville sur l'approximation de nombres algébriques a été considérablement approfondi par les belles recherches de Thue et Siegel. Le résultat principal de Thue peut être exprimé dans la manière suivante : il n'existe qu'un nombre fini de fractions rationnelles $\frac{p}{q}$ pour lesquelles l'inégalité

$$\left|\mathfrak{I} - \frac{p}{q}\right| > \frac{M}{q^{\mu}} \tag{7}$$

n'est pas satisfaite; ici M est une constante positive arbitraire, et $\mu = \frac{n}{2} + 1 + \varepsilon$, $\varepsilon > 0$. Siegel a réussi a prouver que le théorème de Thue est correct même en remplaçant l'exposant μ par $2\sqrt{n}$. Dans le même Mémoire Siegel a aussi généralisé ses considérations à l'approximation d'un nombre algébrique par un autre.

Il est bien connu, je l'observe en passant, que l'on peut toujours trouver pour un nombre réel arbitraire ρ une infinité de fractions rationnelles $\frac{p}{q}$ ayant ρ comme limite et pour lesquelles

$$\left|\rho - \frac{p}{q}\right| < \frac{1}{\sqrt{5}\, q^2}.$$

Ce résultat est dû à Hurwitz, et l'on sait aussi que la constante $\sqrt{5}$ du dénominateur est la meilleure possible; en effet, on peut démontrer que pour le nombre $\rho = \frac{\sqrt{5}+1}{2}$ cette constante ne peut pas être remplacée par une valeur plus grande, c'est à-dire que l'approximation de ce nombre particulier ρ en nombres rationnels est la plus mauvaise possible. Les recherches de Hurwitz ont été continuées par un grand nombre d'auteurs, je vais signaler ici seulement les travaux de Perron [1] et Heawood. Les résultats, quoique très intéressants, ne sont pas directement liés avec la théorie des nombres algébriques et je ne les discuterai pas davantage.

3. Critères pour les nombres algébriques. — Les problèmes d'approximation sont en général traités par des considérations sur les fractions continues. D'après Lagrange, on sait que les irrationnalités quadratiques réelles sont complètement caractérisées par la propriété que le développement correspondant en fraction continue est périodique; c'est alors une idée bien naturelle de chercher des critères analogues pour les nombres algébriques de degrés supérieurs.

On peut considérer le développement d'un nombre en fraction continue comme un procédé récurrent par lequel on peut, de deux nombres donnés, déduire une suite de nombres accouplés représentant les fractions approximatives. Jacobi a considéré les suites récurrentes simultanées pour trois ou plusieurs nombres, et en a déduit un algorithme généralisant les fractions continues. Il est connu que chaque série périodique de Jacobi pour trois nombres correspond à une irrationnalité cubique, mais on ne sait pas inversement si toutes les irrationnalités cubiques ont un développement périodique. Il existe pour des nombres algébriques cubiques de nombreuses recherches spéciales, pour $n > 3$ l'algorithme de Jacobi a été étudié profondément par Perron [2], mais les résultats semblent indiquer, qu'il ne sera pas possible d'y tirer un critère général.

On doit à Minkowski [1] le premier critère général pour les nombres algébriques. La méthode de Minkowski est aussi, on peut le dire, une généralisation des fractions continues. La détermination des fractions approximatives dans le développement d'un nombre α est intimement liée avec l'approximation de la droite $y = \alpha x$ par des points de grillage. Minkowski considère pour un nombre α le plan

$$F(x) = x_0 + x_1 x + \ldots + x_{n-1} x^{n-1} = 0 \tag{8}$$

dans l'espace à n dimensions. Par un procédé simple on définit n minima de $|F(x)|$

$$m_0^{(t)}, \quad m_1^{(t)}, \quad \ldots, \quad m_{n-1}^{(t)} \qquad (t = 1, 2, \ldots) \tag{9}$$

pour les points de grillage contenus dans le carré $|x_i| \leqq t$; le nombre $m_0^{(t)}$ est le minimum absolu de $|F(x)|$ dans ce carré. Il faut et il suffit alors, pour que le nombre α soit algébrique de degré n, que la série (9) soit infinie et que les fractions

$$\frac{m_i^{(t)}}{m_0^{(t)}} \qquad (i = 1, 2, \ldots, n-1, \; t = 1, 2, \ldots)$$

ne prennent qu'un nombre fini de valeurs différentes. Cet algorithme n'est pas en général périodique pour les nombres algébriques, sauf dans des cas très spéciaux déterminés aussi par Minkowski [2]. Un critère semblant fondé sur les idées de Minkowski a été déduit par Furtwängler [1]; ce critère est plus simple que celui de Minkowski, parce que seulement les minima absolus $m_0^{(t)}$ y entrent.

Un critère d'une forme differente a été obtenu par Pipping en généralisant l'algorithme d'Euclide. Soit

$$S^{(1)} = [\nu_0 \geqq \nu_1 \geqq \ldots \geqq \nu_n > 0]$$

un système de $n+1$ nombres réels positifs; de ce système on déduit n systèmes nouveaux $S_i^{(2)}$ en remplaçant toujours le plus grand nombre ν_0 par $\nu_0 - \nu_i$. De la même manière on obtient de $S_i^{(2)}$ les n^2 systèmes $S_i^{(3)}$, ..., et on continuera cet algorithme jusqu'à l'apparition d'un système contenant un nombre égal à zéro. Alors on peut démontrer : le nombre algébrique réel α de degré n est complètement caractérisé par la propriété, que n est le plus petit nombre pour lequel cet algorithme effectué sur les nombres

$$1, \alpha, \ldots, \alpha^{n-1}$$

est fini.

CHAPITRE II.

1. **Les corps algébriques.** — Soit C un système de nombres réels ou complexes; nous appelons C un *corps*, quand le système est *clos par rapport aux quatre opérations élémentaires;* c'est à-dire si α et β sont deux éléments d'un corps C, les nombres $\alpha \pm \beta$, $\alpha\beta$ et $\frac{\alpha}{\beta}(\beta \neq 0)$ seront aussi contenus dans C. On trouve déjà chez Abel des considérations générales sur les corps; j'observe aussi que le corps, notion introduite par Dedekind, est identique au domaine de rationnalité de Kronecker.

Un *anneau* A est un système clos par rapport à l'addition, soustraction et multiplication. Parfois il est utile d'introduire aussi la notion des *modules*, qui sont des systèmes clos par respect à l'addition et soustraction.

Il est évident que l'ensemble des nombres complexes, des nombres

réels et des nombres rationnels sont des corps; de même par exemple les nombres des formes $a + ib$ ou $a + b\sqrt{-3}$ (a, b rationnels). Les nombres entiers ordinaires forment un anneau qui n'est pas en même temps un corps, ainsi que les nombres $a + ib$ ou $a + b\sqrt{-3}$ (a, b entiers). Dans la suite nous allons considérer des exemples nombreux de corps et d'anneaux et une énumération continue sera donc superflue. Je fais seulement observer que tout corps défini ainsi contient le corps R des nombres rationnels; en effet, soit $\alpha \neq 0$ un nombre de C. Alors C doit contenir $\frac{\alpha}{\alpha} = 1$ et par conséquent tous les nombres entiers ainsi que leurs rapports, c'est-à-dire l'ensemble R.

Définition. Un corps algébrique est un corps qui ne contient que des nombres algébriques. — Dans la suite nous allons étudier exclusivement des corps algébriques. Les deux théorèmes suivants sont alors fondamentaux :

L'ensemble de tous les nombres algébriques est un corps.

L'ensemble de tous les nombres algébriques entiers est un anneau.

La démonstration de ces propositions peut être déduite par deux méthodes différentes, qui sont toutes les deux caractéristiques pour beaucoup de problèmes dans cette théorie :

1° Méthode des fonctions symétriques;
2° Méthode de la dépendance linéaire.

La méthode des fonctions symétriques est fondée sur le théorème bien connu : soit $F(\sigma_1, \ldots, \alpha_n)$ une fonction rationnelle entière symétrique des variables σ avec des coefficients contenus dans un corps ou un anneau donné. Alors on a

$$F(\alpha_1, \ldots, \alpha_n) = G(a_1, \ldots, a_n),$$

où G est aussi une fonction entière avec des coefficients du même corps ou anneau, et les a_i sont les fonctions symétriques élémentaires des α_i définies par

$$(t - \alpha_1)\ldots(t - \alpha_n) = t^n + a_1 t^{n-1} + \ldots + a_n.$$

Dans la suite nous supposerons pour la plupart, que $\alpha_1, \ldots, \alpha_n$ sont

des nombres algébriques conjugués et que les coefficients de F sont des nombres rationnels. Alors $F(\alpha_1, \ldots, \alpha_n)$ sera un nombre rationnel et même un nombre entier, si les α_i sont des entiers algébriques et les coefficients de F sont tous entiers.

Supposons alors que α et β sont deux nombres algébriques et que les équations caractéristiques correspondantes $f(x) = 0$, $\varphi(x) = 0$ ont les racines

$$\alpha = \alpha_1, \ldots, \alpha_n, \qquad \beta = \beta_1, \ldots, \beta_m.$$

Le nombre $\alpha + \beta$ est par conséquent une racine de l'équation

$$H(x) = f(x - \beta_1), \ldots, f(x - \beta_m) = 0$$

et cette équation a des coefficients rationnels symétriques dans les β_i; le nombre $\alpha + \beta$ est alors algébrique et de même $\alpha - \beta$. On voit aussi immédiatement que $\alpha \pm \beta$ est entier si α et β ont cette propriété. Le nombre $\alpha\beta$ est une racine de

$$G(x) = (\beta_1 \ldots \beta_m)^n f\left(\frac{x}{\beta_1}\right) \ldots f\left(\frac{x}{\beta_m}\right) = 0$$

et l'on en tire les mêmes conclusions; finalement on observe que $\frac{\alpha}{\beta} = \alpha \frac{1}{\beta}$ et $\frac{1}{\beta}$ est une racine de $\varphi\left(\frac{1}{x}\right) = 0$.

Pour obtenir les mêmes résultats par des considérations sur des systèmes linéaires, on applique le lemme suivant : *soit $\Im$ un nombre arbitraire, et $\omega_1, \omega_2, \ldots, \omega_n$ un système de nombres donnés non tous zéro; alors $\Im$ est un nombre algébrique, si l'on peut exprimer tous les produits $\Im\omega_i$ linéairement par les ω_i avec des coefficients rationnels, et $\Im$ est entier lorsque ces coefficients sont des entiers rationnels.* En effet, supposons qu'une représentation

$$\omega_i \Im = \sum_{j=1}^{n} a_{ij} \omega_j \qquad (i = 1, 2, \ldots, n)$$

aura lieu, on peut pourtant considérer ces équations comme un système homogène en les ω_i et l'on obtient, par conséquent,

$$\begin{vmatrix} a_{11} - \Im & a_{12} & a_{1n} \\ a_{21} & a_{22} - \Im & a_{2n} \\ \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & a_{nn} - \Im \end{vmatrix} = 0$$

et notre lemme est démontré.

Pour en tirer les propriétés indiquées des nombres algébriques mettons

$$\omega_{i,j} = \alpha^i \beta^j \qquad (i = 0, 1, \ldots, n-1; j = 0, 1, \ldots, m-1)$$

et $\mathfrak{Z} = \alpha \pm \beta$ ou bien $\mathfrak{Z} = \alpha\beta$. On voit sans difficulté que tous les produits $\mathfrak{Z}\omega_{ij}$ peuvent être représentés par des expressions linéaires en les ω_{ij}, ce qui donne aussitôt les théorèmes désirés.

Il faut indiquer ici aussi une autre propriété des nombres algébriques : *Toute racine d'une équation*

$$f(x) = x^n + \alpha x^{n-1} + \beta x^{n-2} + \ldots + \delta = 0$$

avec des coefficients algébriques est aussi un nombre algébrique, et même un nombre algébrique entier si tous les coefficients de $f(x)$ *sont entiers.* La démonstration en est facile : Il faut seulement former le produit de $f(x)$ avec tous les polynomes qu'on obtient de $f(x)$ en remplaçant les coefficients α, β, ..., par toutes combinaisons possibles des nombres conjugués. Le produit sera alors symétrique dans les conjugués et aura nécessairement des coefficients rationnels, et des coefficients entiers si les coefficients de $f(x)$ sont des entiers algébriques.

2. **Les corps finis.** — Les corps algébriques les plus simples sont les corps $R(\mathfrak{Z})$ engendrés par un seul nombre algébrique; ce corps consiste de toutes fonctions rationnelles de $\mathfrak{Z}$ avec des coefficients rationnels. Il est évident que tous ces nombres constituent un corps, et nous disons que $R(\mathfrak{Z})$ est produit par l'*adjonction* du nombre $\mathfrak{Z}$ au corps R des nombres rationnels.

On peut représenter un nombre arbitraire de $R(\mathfrak{Z})$ dans la forme

$$\alpha = \frac{F(\mathfrak{Z})}{G(\mathfrak{Z})}, \tag{1}$$

où $F(x)$ et $G(x)$ sont des polynomes, et $\mathfrak{Z}$ est une racine de l'équation caractéristique

$$(2)\quad f(x) = x^n + a_1 x^{n-1} + \ldots + a_n = (x - \mathfrak{Z})(x - \mathfrak{Z}^{(1)}) \ldots (x - \mathfrak{Z}^{(n)}) = 0.$$

Nous appelons le nombre n le *degré* de $R(\mathfrak{Z})$. On peut cependant toujours représenter le nombre α en (1) dans une forme réduite

unique; en effet, les polynomes $f(x)$ et $G(x)$ n'ont pas de facteur commun, parce que $G(\mathfrak{I}) \neq 0$, et l'on peut, d'après un théorème bien connu, déterminer les polynomes $A(x)$ et $B(x)$ à coefficients rationnels de manière que

$$A(x)f(x) + B(x)G(x) = 1,$$

d'où l'on tire $G(\mathfrak{I})^{-1} = B(\mathfrak{I})$. Le nombre α est donc égal à un polynome en $\mathfrak{I}$, et en divisant ce polynome par $f(x)$ ou, ce qui est la même chose, en réduisant les puissances supérieures de $\mathfrak{I}$ par la relation

$$\mathfrak{I}^n = -(a_1\mathfrak{I}^{n-1} + \ldots + a_n), \tag{3}$$

on obtient

$$\alpha = \alpha(\mathfrak{I}) = b_0 + b_1\mathfrak{I} + \ldots + b_{n-1}\mathfrak{I}^{n-1}. \tag{4}$$

Cette représentation de α est unique, parce que de deux représentations différentes on trouvera une équation de degré $< n$ pour $\mathfrak{I}$.

Tous les nombres $\alpha(\mathfrak{I})$ en $R(\mathfrak{I})$ sont des nombres algébriques de degré $\leq n$; en effet, α doit satisfaire à l'équation

$$h(x) = [x - \alpha(\mathfrak{I})][(x - \alpha(\mathfrak{I}^{(2)})]\ldots[x - \alpha(\mathfrak{I}^{(n)})] = 0, \tag{5}$$

qui a évidemment des coefficients rationnels. $\alpha(\mathfrak{I})$ est dit *nombre primitif* de $R(\mathfrak{I})$ s'il satisfait à une équation irréductible de degré n, c'est-à-dire l'équation (5) doit être irréductible.

Pour que le nombre α soit primitif, il faut et il suffit que les nombres

$$\alpha(\mathfrak{I}), \quad \alpha(\mathfrak{I}^{(2)}), \quad \ldots, \quad \alpha(\mathfrak{I}^{(n)}) \tag{6}$$

en (5) soient tous différents. Supposons, en effet, que $d(x) = 0$ soit l'équation caractéristique de $\alpha(\mathfrak{I})$; alors on a $d[\alpha(\mathfrak{I})] = 0$, d'où l'on tire

$$d[\alpha(x)] = f(x)\,q(x),$$

$q(x)$ étant un polynome. En remplaçant dans cette identité x par les $\mathfrak{I}^{(i)}$ on voit que tous les nombres (6) sont des racines de $d(x) = 0$, c'est-à-dire $d(x)$ est au moins de degré n et l'on a $d(x) = h(x)$.

Même dans le cas où quelques-uns des nombres (6) sont égaux, il

s'ensuit que l'équation $d(x) = 0$ est satisfaite par tous les nombres différents. On peut donc écrire

$$h(x) = d(x)^a d_1(x),$$

où $d_1(x)$ n'est pas divisible par $d(x)$. A l'autre côté toutes les racines de $d_1(x) = 0$ sont contenues entre les nombres (6) qui sont aussi des racines de $d(x) = 0$, et l'on aura nécessairement $d_1(x) = 1$ et

$$h(x) = d(x)^a. \tag{7}$$

Nous avons donc démontré : *Tous les nombres du corps* $R(\mathfrak{Z})$ *sont des nombres algébriques dont les degrés sont des diviseurs du degré n du corps.*

Tous les nombres rationnels sont des nombres imprimitifs dans $R(\mathfrak{Z})$; si les nombres rationnels sont les seuls éléments imprimitifs, on dit que *le corps* $R(\mathfrak{Z})$ *est primitif*. Il est évident que $R(\mathfrak{Z})$ est un corps primitif si le degré n est un nombre premier.

3. **Les éléments primitifs.** — Nous allons montrer que les corps $R(\mathfrak{Z})$ et $R(\alpha)$ sont identiques si α est un élément primitif de $R(\mathfrak{Z})$. Il suffit d'exprimer le nombre $\mathfrak{Z}$ en fonction rationnelle de α; dans ce but nous construisons le polynome

$$H(x) = h(x)\left(\frac{\mathfrak{Z}}{x - \alpha(\mathfrak{Z})} + \frac{\mathfrak{Z}^{(2)}}{x - \alpha(\mathfrak{Z}^{(1)})} + \ldots + \frac{\mathfrak{Z}^{(n)}}{x - \alpha(\mathfrak{Z}^{(n)})}\right),$$

où $h(x)$ est le polynome caractéristique de $\alpha(\mathfrak{Z})$. On voit aussitôt que $H(x)$ a des coefficients rationnels et pour $x = \alpha$ on obtient sans difficulté

$$H(\alpha) = h'(\alpha)\mathfrak{Z}\,(^1).$$

On peut aussi déduire tous ces résultats sur le corps $R(\mathfrak{Z})$ par des considérations linéaires et, pour les calculs numériques, cette dernière méthode est en général préférable.

Soit α un nombre donné par (4); de (3) on en déduit, de proche

(1) Il faut observer que la notion du dérivé dans l'algèbre peut être introduite par des considérations parfaitement normales sans application des passages à la limite.

en proche, les relations

$$(8)\qquad \begin{cases} \alpha = b_{0,0} + b_{1,0}\Im + \ldots + b_{n-1,0}\Im^{n-1}, \\ \Im\alpha = b_{0,1} + b_{1,1}\Im + \ldots + b_{n-1,1}\Im^{n-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ \Im^{n-1}\alpha = b_{0,n-1} + b_{1,n-1}\Im + \ldots + b_{n-1,n-1}\Im^{n-1}, \end{cases}$$

d'où l'on tire l'équation cherchée

$$(9)\qquad \begin{vmatrix} b_{0,0}-\alpha & b_{1,0} & \ldots & b_{n-1,0} \\ b_{0,1} & b_{1,1}-\alpha & \ldots & b_{n-1,1} \\ \ldots & \ldots\ldots & \ldots & \ldots\ldots \\ b_{0,n-1} & b_{1,n-1} & \ldots & b_{n-1,n-1}-\alpha \end{vmatrix} = 0.$$

Si α est un nombre primitif, il ne peut pas satisfaire à une équation de degré inférieur à n et les mineurs d'ordre $n-1$ du déterminant (9) ne sont pas tous nuls. On peut par conséquent tirer de (8) la valeur de $\Im$ exprimée rationnellement par α.

Nous avons jusqu'à présent considéré seulement les corps simples engendrés par un seul nombre algébrique. On peut naturellement étudier les corps plus généraux $R(\alpha, \beta)$ engendrés par deux nombres ou bien $R(\alpha, \beta, \ldots, \delta)$ engendrés par un nombre arbitraire de nombres algébriques. Le corps $R(\alpha, \beta)$ consiste par exemple par toutes les fonctions rationnelles de α et β avec des coefficients rationnels.

Il existe pour les corps $R(\alpha, \beta, \ldots, \delta)$ obtenus par un nombre fini d'adjonctions un théorème important, le *théorème de l'élément primitif*. *Tout corps* $R(\alpha, \beta, \ldots, \delta)$ *est équivalent à un corps simple* $R(\Im)$, c'est-à-dire, on peut trouver un nombre primitif $\Im$ dans $R(\alpha, \beta, \ldots, \delta)$ de sorte que tous les nombres de ce corps peuvent être exprimés rationnellement par $\Im$.

Il suffit d'établir ce théorème pour un corps $R(\alpha, \beta)$. Nous mettons $\xi = \alpha + k\beta$, où k est un nombre rationnel; on voit alors que ξ est un nombre de $R(\alpha, \beta)$, et, en nous servant des mêmes notations qu'auparavant, que ξ satisfait à l'équation

$$F(x) = \prod_{i,j=1}^{n,m} (x - \xi_{i,j}) = 0, \qquad \xi_{i,j} = \alpha_i + k\beta_j,$$

à coefficients rationnels. Nous choisissons à présent k de sorte que toutes les racines $\xi_{i,j}$ soient différentes, ce qui est toujours possible.

Soit alors $A(\alpha, \beta)$ un nombre arbitraire de $K(\alpha, \beta)$; nous considérons le polynome

$$H(t) = \sum_{i,j=1}^{n,m} \frac{A(\alpha_i, \beta_j)}{t - \xi_{i,j}} F(t),$$

qui a des coefficients rationnels, étant symétrique en les α_i et β_j. Pour $t = \xi$ on obtient comme autrement

$$A(\alpha, \beta) = \frac{H(\xi)}{F'(\xi)}.$$

Le théorème de l'élément primitif nous donne une classification importante des corps algébriques : Les corps engendrés par un nombre fini d'adjonctions, c'est-à-dire les corps simples $R(\mathfrak{I})$, s'appellent *corps algébriques finis;* les corps qu'on peut obtenir seulement par un nombre infini d'adjonctions s'appellent *corps algébriques infinis*. Dans la suite nous allons étudier principalement les corps finis; comme exemple de corps infinis je veux citer les corps des nombres algébriques réels : Les corps contenant tous les nombres exprimables, soit par racines carrées, soit par des radicaux arbitraires. sont aussi des corps infinis.

4. **Norme, discriminant, systèmes linéaires.** — Revenons au corps simple $R(\mathfrak{I})$; nous avons vu que les nombres différents dans le système (6) sont les racines de l'équation caractéristique de α, et les nombres sont donc les conjugués de α au sens défini auparavant. S'il n'y a que m nombres différents dans (6), il s'ensuit de (7) que les nombres (6) se répartissent en a systèmes identiques, chacun contenant les mêmes m nombres différents.

Il faut introduire à ce point quelques notions fondamentales de la théorie des corps algébriques. Les deux expressions

$$N(\alpha) = \alpha(\mathfrak{I})\,\alpha(\mathfrak{I}^{(2)})\ldots\alpha(\mathfrak{I}^{(n)}),$$
$$S(\alpha) = \alpha(\mathfrak{I}) + \alpha(\mathfrak{I}^{(2)}) + \ldots + \alpha(\mathfrak{I}^{(n)})$$

s'appellent respectivement la *norme* et la *trace* de α. $N(\alpha)$ et $S(\alpha)$ sont des nombres rationnels, et même entiers, si α est un nombre algébrique entier. On vérifie sans difficulté que

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

et pour un nombre rationnel a on a

$$N(a) = a^n, \quad S(a) = na.$$

Si α est un nombre primitif satisfaisant à

$$h(x) = x^n + b_1 x^{n-1} + \ldots + b_n = 0, \tag{10}$$

on voit que

$$S(\alpha) = -b_1, \qquad N(\alpha) = (-1)^n b_n,$$

et si $h(x)$ est donné sous la forme (9) on obtient

$$S(\alpha) = b_{0,0} + b_{1,1} + \ldots + b_{n-1,n-1}, \qquad N(\alpha) = |b_{i,j}| \tag{11}$$
$$(i, j = 0, 1, \ldots, n-1).$$

Soient encore

$$\alpha_1, \quad \alpha_2, \quad \ldots, \quad \alpha_n, \tag{12}$$

n nombres du corps et mettons

$$\alpha_k^{(i)} = \alpha_k(\mathfrak{J}^{(i)}) \qquad (i = 1, 2, \ldots, n),$$

alors le *discriminant* du système (12) est défini par

$$\Delta(\alpha_1, \ldots, \alpha_n) = \begin{vmatrix} \alpha_1^{(1)} & \alpha_2^{(1)} & \ldots & \alpha_n^{(1)} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_1^{(n)} & \alpha_2^{(n)} & \ldots & \alpha_n^{(n)} \end{vmatrix}^2 \tag{13}$$

Le discriminant est rationnel, et entier si tous les α_i sont entiers.

Le discriminant $D(\alpha)$ d'un nombre α est le discriminant du système spécial

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

Il est bien connu que

$$D(\alpha) = \begin{vmatrix} 1 & \alpha & \ldots & \alpha^{n-1} \\ 1 & \alpha^{(2)} & \ldots & \alpha^{(2)n-1} \\ \cdot & \ldots & \ldots & \ldots \\ 1 & \alpha^{(n)} & \ldots & \alpha^{(n)n-1} \end{vmatrix}^2 = \prod_{i<j} (\alpha^{(i)} - \alpha^{(j)})^2. \tag{14}$$

La condition nécessaire et suffisante pour que α soit un nombre primitif, est $D(\alpha) \neq 0$; si α est primitif, $D(\alpha)$ est le discriminant de l'équation caractéristique (10).

La *différente* d'un nombre primitif α est

$$h'(\alpha) = (\alpha - \alpha^{(2)}) \ldots (\alpha - \alpha^{(n)}); \tag{15}$$

de (14), (15) et de la définition de la norme on tire sans difficulté la relation suivante entre le discriminant et la différente :

$$D(\alpha) = (-1)^{\frac{1}{2}n(n-1)} N[h'(\alpha)] \tag{16}$$

Le discriminant d'un système (12) a une signification importante que nous allons déduire. Nous disons que les r nombres du corps

$$\beta_1, \quad \beta_2, \quad \ldots, \quad \beta_r, \tag{17}$$

sont linéairement indépendants si une relation

$$b_1\beta_1 + b_2\beta_2 + \ldots + b_r\beta_r = 0, \tag{18}$$

les b_i étant rationnels, ne peut pas exister sauf dans le cas

$$b_1 = \ldots = b_r = 0.$$

Si α est un nombre primitif le système $1, \alpha, \ldots, \alpha^{n-1}$ est linéairement indépendant.

On peut montrer : *Un système linéairement indépendant du corps contient au plus n nombres.* En effet, on exprime les r nombres (17) linéairement par les puissances $1, \mathfrak{Z}, \ldots, \mathfrak{Z}^{n-1}$, et la condition (18) nous donne n équations linéaires et homogènes pour les b_i. Si $r > n$ on sait, d'après un théorème bien connu, qu'on peut toujours trouver une solution de ce système tel que les b_i ne soient pas tous nuls.

Nous avons vu que chaque nombre du corps a une représentation unique (4); si un système (17) a la propriété qu'un nombre quelconque du corps peut être representé dans une manière unique sous la forme

$$\omega = b_1\beta_1 + \ldots + b_r\beta_r,$$

on dit que les nombres (17) forment une *base* du corps. On peut alors démontrer : *Une base est un système de n nombres linéairement indépendants du corps.* Le nombre O ayant une représentation unique, il s'ensuit que les β_i sont linéairement indépendants; si l'on exprime les produits $\omega\beta_i$ linéairement par les β_i on voit d'après un lemme du paragraphe 1, que le nombre ω doit toujours satisfaire à une équation de degré $\leq r$, d'où l'on obtient $n = r$. A l'autre côté, soit

$$\beta_1, \quad \beta_2, \quad \ldots, \quad \beta_n \tag{19}$$

un système de n nombres linéairement indépendants. Si ω est un nombre arbitraire du corps, les $n+1$ nombres $\omega, \beta_1, \ldots, \beta_n$ sont nécessairement dépendants et l'on en déduit une représentation linéaire de ω par les β_i. Le système (19) est donc une base.

Soit d'ailleurs $\gamma_i (i = 1, 2, \ldots, n)$ une base différente du corps; on peut alors représenter les nombres de la base (19) linéairement par les γ_i

$$\beta_i = \sum_{j=1}^{n} c_{i,j}\gamma_j \qquad (i = 1, 2, \ldots, n). \tag{20}$$

Réciproquement on peut aussi représenter les γ_i par les β_i et il faut donc que $|c_{ij}| \neq 0$, et de la définition du discriminant on obtient la relation suivante

$$\Delta(\beta_1 \ldots \beta_n) = |c_{ij}|^2 \Delta(\gamma_1 \ldots \gamma_n) \tag{21}$$

entre les discriminants de deux bases.

Nous démontrerons finalement : *Il faut et il suffit pour qu'un système* (19) *soit une base, que le discriminant du système ne soit pas nul.* Nous avons vu, en effet, qu'un système (19) est une base seulement si l'on peut exprimer les nombres β_i par une base γ_i tel que le déterminant de la représentation ne soit pas nul. Prenons pour la base $1, \vartheta, \ldots, \vartheta^{n-1}$ dont le discriminant n'est pas nul: on en tire que le discriminant des β_i et le déterminant de $|c_{ij}|$ sont en même temps nuls ou différents de nul.

D'après (21) tous les discriminants du corps ont le même signe. Il résulte de (14) que ce signe est

$$(-1)^r = (-1)^{\frac{n-r}{2}},$$

où r représente le nombre de racines réelles et $2c$ le nombre de racines complexes de l'équation (2) définissant le corps (*Hensel*) [1].

5. **Bases minimales.** — Il existe dans un corps donné $R(\vartheta)$ toujours des *bases entières*, c'est-à-dire des bases (19) dans lesquelles tous les nombres β_i sont entiers. On peut en effet, d'après le paragraphe 1, Chapitre I, trouver un nombre m tel que tous les produits $m\beta_i$ sont entiers.

Le discriminant d'une base entière est un nombre rationnel entier, et entre toutes les bases entières il en existe donc au moins une, pour

laquelle le discriminant a une valeur absolue minimale $|d|$. Ce discriminant minimal d est appelé le *nombre fondamental* ou plus souvent *le discriminant du corps*.

Les bases ayant le discriminant d sont des *bases minimales*, et elles sont aussi caractérisées par la propriété suivante : *Soit*

$$\omega_1, \omega_2, \ldots, \omega_n, \qquad \Delta(\omega_1 \ldots \omega_n) = d, \tag{22}$$

une base minimale. Chaque nombre entier ω *du corps et seulement les entiers peuvent être représentés sous la forme*

$$\omega = a_1\omega_1 + \ldots + a_n\omega_n, \tag{23}$$

avec des coefficients rationnels entiers.

Tous les nombres (23) sont entiers et il faut seulement prouver qu'il n'existe aucun entier

$$\bar{\omega} = b_1\omega_1 + \ldots + b_n\omega_n$$

avec coefficients non entiers b_i. Supposons d'abord que $b_1 = a + r$, où a est entier et $0 < r < 1$ une fraction rationnelle. Alors $\bar{\bar{\omega}} = \bar{\omega} - a\omega_1$ est aussi entier, et les nombres

$$\bar{\bar{\omega}}_1, \quad \omega_2, \quad \ldots, \quad \omega_n$$

forment, comme on le voit facilement d'après (21), une base entière avec le discriminant $r^2 d$, ce qui est impossible d'après la définition d'une base minimale.

Cette démonstration, quoique très élégante, ne donne aucune méthode pour la détermination actuelle d'une base minimale; nous allons montrer comment on peut, d'une base entière quelconque, déduire une base minimale. Soit (19) la base entière donnée, par exemple les puissances d'un nombre primitif entier du corps. Soit D le discriminant de cette base et

$$\omega = a_1\beta_1 + \ldots + a_n\beta_n \tag{24}$$

la représentation d'un nombre entier ω. De (24) on déduit des relations analogues pour les nombres conjugués

$$\omega^{(i)} = a_1\beta_1^{(i)} + \ldots + a_n\beta_n^{(i)}, \tag{25}$$

et le déterminant de ce système linéaire dans les a_i est $\sqrt{D}$. On obtient

en éliminant

$$a_\iota = \frac{b_\iota}{D},$$

où b_ι est nécessairement un nombre algébrique entier, ce qui s'ensuit de la représentation de b_ι par des déterminants. b_ι est alors aussi un nombre rationnel entier, et il existe donc toujours une représentation

$$\omega = \frac{b_1\beta_1 + \ldots + \beta_n}{D}. \tag{26}$$

Pourtant, tous nombres de cette forme ne sont pas inversement des entiers; soit ω un nombre (26) arbitraire; en divisant les b_ι par D on obtient

$$\omega = \gamma + \rho,$$

où γ est entier et ρ un nombre de la forme (26) avec

$$0 \leqq b_\iota < D \ (\iota = 1, 2, \ldots, n).$$

Il n'y a qu'un nombre fini des ρ et en construisant les équations correspondantes on trouve les nombres *entiers* $\rho_1, \ldots, \rho_k$ entre eux; le caractère d'un nombre (26) est donc simple à constater. Considérons alors pour $m = 1, 2, \ldots, n$ tous les nombres entiers de la forme

$$\omega_m = \frac{b_{1,m}\beta_1 + \ldots + b_{m,m}\beta_m}{D}. \tag{27}$$

En considérant les ρ_ι de cette forme, on peut déterminer un $\bar{\omega}_m$ ayant la propriété que le coefficient $\bar{b}_{m,m} > 0$ est aussi petit que possible. Ce coefficient $\bar{b}_{m,m}$ est un diviseur de tous les $b_{m,m}$ des entiers (27) parce que, au cas contraire, on trouverait un $\bar{b}_{m,m}$ encore plus petit. Les nombres

$$\bar{\omega}_1, \quad \bar{\omega}_2, \quad \ldots, \quad \bar{\omega}_n$$

ainsi définis forment une base minimale. En effet, dans la représentation (26) d'un entier ω, le coefficient b_n est divisible par $\bar{b}_{n,n}$, par conséquent $b_n = a_n\bar{b}_{n,n}$. Alors $\omega - a_n\bar{\omega}_n$ est un nombre (27) avec $m = n - 1$. De la même manière on obtient, pour ce nombre, $b_{n-1,n-1} = a_{n-1}\bar{b}_{n-1,n-1}$ et ainsi de suite.

Cette méthode, quoique praticable, est ordinairement très fatigante. On peut souvent l'abréger en appliquant des résultats de la théorie

des idéaux; je fais mention aussi des recherches de *W. E. H. Berwick* qui nous permettent, sinon toujours, du moins dans beaucoup de cas, de réduire considérablement le travail requis. Il existe de nombreuses recherches sur les bases des corps spéciaux, par exemple les corps de degré $n = 2, 3, 4$, les corps binomiaux, les corps de racines d'unité, etc.

Pour les corps quadratiques la détermination d'une base est très facile. Le nombre général d'un corps quadratique a la forme $\vartheta = a + b\sqrt{D}$ où a et b sont rationnels et D est un entier rationnel sans facteurs carrés. L'équation caractéristique de ϑ est

$$x^2 - 2ax + a^2 - Db^2 = 0,$$

et en trouvant la condition pour des coefficients entiers on déduit les bases

$$\omega_1 = 1, \quad \omega_2 = \sqrt{D} \qquad \text{pour } D \equiv 2 \text{ ou } D \equiv 3 \pmod 4,$$

$$\omega_1 = 1, \quad \omega_2 = \frac{1 + \sqrt{D}}{2} \qquad \text{pour } D \equiv 1 \pmod 4.$$

Le discriminant d'un corps quadratique $R(\sqrt{D})$ est donc $d = 4D$ ou $d = D$ selon que $D \equiv 2$, 3 ou $D \equiv 1 \pmod 4$. On peut montrer, même pour un corps général, l'existence d'une base minimale avec $\omega_1 = 1$.

6. **Théorèmes de Minkowski.** — Le discriminant d'un corps a des propriétés diverses, qui sont pour la plupart étroitement liées avec les propriétés arithmétiques du corps. Je vais donc faire mention ici seulement du théorème célèbre de *Minkowski :*

Si d est le discriminant d'un corps de degré $n > 1$, on a toujours

$$|d| > 1. \tag{28}$$

Ce résultat est une conséquence d'un autre théorème de *Minkowski* [3] sur des formes linéaires, un théorème très utile dans beaucoup de recherches dans la théorie des nombres algébriques :

Soit

$$L_a(x) = \sum_{b=1}^{n} A_{a,b} x_b \qquad (a = 1, 2, \ldots, n), \tag{29}$$

un système de formes linéaires à coefficients réels tel que le déter-

minant $D = |A_{a,b}|$ *ne soit pas nul; soit davantage* $d_1, d_2, \ldots, d_n$, *n nombres réels positifs satisfaisant à la condition*

$$d_1 d_2 \ldots d_n \geqq |D|. \tag{30}$$

Alors on peut toujours trouver un système de n nombres rationnels entiers $x_1^{(0)}, x_2^{(0)}, \ldots, x_n^{(0)}$, *qui ne sont pas tous nuls, de manière à faire*

$$|L_a(x^{(0)})| \leqq d_a \qquad (a = 1, 2, \ldots, n). \tag{31}$$

On peut même supposer, que l'inégalité aura lieu dans (31) pour tous $a = 1, 2, \ldots$ sauf pour une seule forme: cette remarque est d'importance dans la suite. Le théorème de Minkowski est aussi vrai pour des formes à coefficients *complexes*, si le système (29) contient toujours en même temps une forme $L_k(x)$ et sa conjuguée

$$L(x) = L_{k+1}(x),$$

et dans ce cas il faut naturellement que $d_k = d_{k+1}$. On réduit ce cas au cas précédent en considérant un système nouveau obtenu de (29) en remplaçant $L_k(x)$ et $L_{k+1}(x)$ par les formes réelles

$$L'_k(x) = \frac{1}{\sqrt{2}}[L_k(x) + L_{k+1}(x)], \qquad L''_k(x) = \frac{1}{i\sqrt{2}}[L_k(x) - L_{k+1}(x)].$$

Le déterminant de ce système est aussi D, et l'on a

$$|L_k(x)| = |L_{k+1}(x)| = \frac{1}{\sqrt{2}}|\sqrt{|L'_k(x)|^2 + |L''_k(x)|^2}| < d_k,$$

en supposant

$$|L'_k(x)| \leqq d_k, \qquad |L''_k(x)| < d_k.$$

Soit d'abord

$$\omega = x_1\omega_1 + x_2\omega_2 + \ldots + x_n\omega_n, \tag{32}$$

la représentation d'un entier arbitraire du corps par une base minimale, et par conséquent

$$\omega^{(i)} = x_1\omega_1^{(i)} + x_2\omega_2^{(i)} + \ldots + x_n\omega_n^{(i)} \qquad (i = 1, 2, \ldots, n) \tag{33}$$

les conjugués de ω. Le déterminant du système (33) est $\pm\sqrt{d}$, et l'on peut donc déterminer, d'après le théorème indiqué, les entiers rationnels x_i de sorte que

$$|\omega^{(i)}| \leqq |\sqrt[2n]{d}| \qquad (i = 1, 2, \ldots, n),$$

où l'inégalité aura lieu pour quelques i. Il existe donc un entier $\omega \neq 0$ du corps tel que $|N(\omega)| < |\sqrt{d}|$, ce qui nous donne $|d| > 1$.

Par des considérations plus profondes, Minkowski a démontré que

$$|d| > \left(\frac{\pi}{4}\right)^{s} \left(\frac{n^n}{n!}\right)^2, \tag{34}$$

où $2c$ représente comme auparavant le nombre de corps conjugués complexes de $R(\mathfrak{I})$.

Nous démontrerons finalement un théorème d'Hermite :

Il n'existe qu'un nombre fini de corps à discriminant donné d.

De (34) il s'ensuit, que le degré d'un corps avec le discriminant d est limité. Nous allons démontrer qu'il existe toujours dans un corps de degré n et discriminant d un nombre *primitif* ω tel que les valeurs absolues des conjugués de ω satisfont aux inégalités

$$|\omega^{(i)}| < M_i \qquad (i = 1, 2, \ldots, n), \tag{35}$$

où les constantes M_i ne dépendent que de d. Le théorème d'Hermite est alors une conséquence directe du lemme suivant :

Il n'existe qu'un nombre fini d'entiers algébriques ω de degré n de sorte que $|\omega^{(i)}| < M$ $(i = 1, 2, \ldots, n)$, M étant une constante donnée.

On obtient en effet pour les coefficients a_i des équations correspondantes les limites

$$|a_i| < \binom{n}{i} M^i (i = 2, \ldots, n).$$

Pour trouver dans un corps de discriminant d un entier primitif pour lequel (35) est satisfait, supposons premièrement que le corps $R(\mathfrak{I})$ est réel. D'après le théorème de Minkowski, on peut alors déterminer les x_i en (32) tel que $|\omega^{(i)}| < 1 (i = 2, \ldots, n)$ et $|\omega| = |\omega^{(1)}| \leqq |\sqrt{d}|$. Puisque la norme de ω est entière, il faut que $|\omega| > 1$, et ω est donc un nombre primitif du corps, étant différent de tous ses conjugués (*voir* § 2). Si $R(\mathfrak{I})$ est un corps complexe, on peut déterminer ω tel que

$$|\omega^{(1)}| = |\omega^{(2)}| \leqq |\sqrt[4]{d}|, \qquad |\omega^{(i)}| < 1 \qquad (i = 3, 4, \ldots, n).$$

On voit facilement, d'après les considérations précédentes sur les formes complexes, qu'on peut faire la partie purement imaginaire de ω différent de zéro, et ω sera donc encore différent de tous ses conjugués.

CHAPITRE III.

1. **Les unités. Racines d'unité.** — Nous disons qu'un entier α du corps K est *divisible* par un autre entier β, si l'on peut déterminer l'entier γ de sorte que $\alpha = \beta\gamma$. *Une unité est un entier du corps divisant tous les nombres de* K.

On peut aussi définir les unités dans des manières différentes :

Une unité ε *est un entier tel que* $\eta = \varepsilon^{-1}$ *est aussi entier.* Dans ce cas $\varepsilon\eta = 1$, ét ε est un diviseur de 1 et par conséquent de tous les nombres de K.

Une unité est un entier tel que

$$\mathrm{N}(\varepsilon) = \pm 1. \tag{1}$$

En effet, de $\varepsilon\eta = 1$ on obtient $\mathrm{N}(\varepsilon)\mathrm{N}(\eta) = 1$, et $\mathrm{N}(\varepsilon) = \pm 1$. De (1) on obtient réciproquement $\varepsilon\eta = 1$, où $\eta = \pm \varepsilon^{(2)} \ldots \varepsilon^{(n)}$ est un entier contenu dans le corps. De (1) il résulte que le produit $\varepsilon_1\varepsilon_2$ et le quotient $\frac{\varepsilon_1}{\varepsilon_2}$ de deux unités sont aussi des unités.

On dit parfois que deux nombres α et β sont *associés*, en signe $\alpha \sim \beta$, si $\alpha = \varepsilon\beta$ où ε est une unité. On voit sans difficulté que $\alpha \sim \alpha$ et que $\beta \sim \alpha$, si $\alpha \sim \beta$; de $\alpha \sim \beta \sim \gamma$ il s'ensuit que $\alpha \sim \gamma$. Si $\alpha \sim \beta$ on a d'après (1)

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

mais cette condition ne suffira pas pour conclure réciproquement que $\alpha \sim \beta$. Considérons à titre d'exemple les unités des corps quadratiques $\mathrm{K}(\sqrt{\mathrm{D}})$; un entier arbitraire a la forme

$$\omega = a + b\sqrt{\mathrm{D}}, \qquad \text{ou} \qquad \omega = a + b\frac{1+\sqrt{\mathrm{D}}}{2} \qquad (a, b \text{ entiers})$$

selon que $\mathrm{D} \equiv 2, 3$ ou $\mathrm{D} \equiv 1 \pmod 4$ (*voir* Chap. II, § 5). La condi-

tion pour une unité sera donc, d'après (1),

$$(2) \qquad a'-b'\mathrm{D}=\pm 1, \qquad \text{ou} \qquad a'+ab+\frac{b^2}{4}(1-\mathrm{D})=\pm 1.$$

Si $\mathrm{K}(\sqrt{\mathrm{D}})$ est un corps quadratique imaginaire, c'est-à-dire $\mathrm{D}<0$, on voit que les seules solutions de (2) sont $a=\pm 1$, $b=0$, sauf dans le cas $\mathrm{D}=-1$, où l'on a en addition la solution $a=0$, $b=\pm 1$ et dans le cas $\mathrm{D}=-3$ où il y a aussi les solutions $a=\pm 1$, $b=\pm 1$. Il résulte donc : *Un corps quadratique imaginaire* $\mathrm{K}(\sqrt{\mathrm{D}})$ *ne contient que les deux unités triviales* $\varepsilon=\pm 1$, *sauf les deux exceptions :* $\mathrm{K}(i)$ *où* $\varepsilon=\pm i$ *et* $\mathrm{K}(\sqrt{-3})$ *où* $\varepsilon=\frac{\pm 1\pm\sqrt{-3}}{2}$. Nous allons voir que les corps quadratiques imaginaires sont les seuls corps qui ne contiennent qu'un nombre *fini* d'unités. Dans les corps quadratiques réels il y a toujours une infinité d'unités, par exemple, dans le corps $\mathrm{K}(\sqrt{2})$ toutes les unités ont la forme $\eta=\pm\varepsilon^a$, où $\varepsilon=1+\sqrt{2}$.

Les racines d'unité, c'est-à-dire les nombres algébriques définis par une équation $x^l=1$, forment une classe d'unité spéciale dans le corps. Il est évident que ces nombres sont toujours des unités, parce que de $\eta^l=1$ on obtient $\eta^{-1}=\eta^{l-1}$. Il est d'importance de noter : *Il n'y a qu'un nombre fini de racines d'unité contenues dans un corps donné* K. Les valeurs absolues des conjugués de η sont limitées, savoir égales à 1, et d'apres un lemme (Chap. II, § 6), il n'y a qu'un nombre fini d'entiers algébriques ayant cette propriété pour un degré donné m. Mais le degré de η est aussi limité, η étant un élément du corps K.

Si ε et η sont des racines primitives de $x^l=1$ et $x^m=1$ respectivement, on voit que $\varepsilon\eta$ est une racine primitive de $x^{\frac{lm}{d}}=1$, $d=(l,m)$. Il existe donc un nombre M tel que les racines d'unité contenues dans K sont toutes les racines de

$$(3) \qquad x^{\mathrm{M}}-1=0.$$

Ces résultats sont aussi des conséquences immédiates du théorème suivant (Ore) [2] :

Toutes les racines d'unité contenues dans K *satisfont à l'équation*

$$x^{\circ d}=1,$$

où d est le discriminant du corps.

Le nombre M en (3) est donc un diviseur de $2d$. La démonstration de ce théorème est basée sur des propriétés simples des corps relatifs. Il est bien connu qu'une racine primitive de (3) satisfait à une équation irréductible de degré $\varphi(M)$ où φ est la fonction d'Euler; d'après le Chapitre II (§ 2), $\varphi(M)$ est donc un diviseur du degré n de K.

Tout corps contient des racines d'unité triviales ± 1. S'il en contient d'autres, il faut que K et tous ses corps conjugués soient imaginaires. En effet, une racine primitive d'unité est toujours complexe ainsi que tous les nombres conjugués.

Je vais faire mention finalement d'un théorème de *Kronecker* qui est étroitement lié avec ces recherches : *Tout entier algébrique pour lequel les valeurs absolues des conjugués sont toutes égales à* 1, *est une racine d'unité*. Si η est un tel entier, on voit comme auparavant qu'il n'y a qu'un nombre fini des η de degré donné, les valeurs absolues des conjugués de η étant limitées. A l'autre côté, toutes les puissances de η ont la même propriété et l'on obtient donc pour quelques a et b

$$\eta^a = \eta^b, \qquad \eta^{a-b} = 1.$$

2. Divisibilité des nombres algébriques. — La théorie des nombres algébriques a été développée par Gauss, Dirichlet et Kummer avant tout pour les applications à la théorie des nombres. De ce point de vue les propriétés des nombres algébriques à l'égard de divisibilité et factorisation sont d'une importance fondamentale; malheureusement la théorie arithmétique des nombres algébriques est, en plusieurs rapports, plus compliquée que pour les nombres rationnels.

Nous avons défini que α est divisible par β si $\alpha = \beta\gamma$ (1). Un nombre α est donc divisible par toutes les unités et par tous les nombres associés; nous appelons *nombre primaire* un nombre π qui ne contient que ces facteurs. On peut alors montrer qu'*il existe pour chaque nombre* α *au moins une décomposition en facteurs primaires*. En effet, si α n'est pas primaire, on a $\alpha = \beta\gamma$, où ni β, ni γ n'est une unité; alors on a

$$N(\alpha) = N(\beta)N(\gamma) \qquad \text{et} \qquad 1 < |N(\beta)| < |N(\alpha)|$$

et de même pour γ. Si β et γ ne sont pas tous les deux nombres pri-

(1) Il s'agit dans la suite seulement des nombres entiers.

maires, on peut effectuer encore une décomposition et ainsi de suite. Ce procédé finira par nous donner une décomposition en facteurs primaires parce que les normes des facteurs ne peuvent pas diminuer sans limites.

Cette décomposition en facteurs primaires n'est pas en général unique. Pour en donner un exemple considérons la décomposition du nombre 21 dans le corps $K(\sqrt{-5})$; d'après le paragraphe 1. ce corps ne contient que les unités triviales ± 1. On a

$$21 = 3.7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$$

et aucun des facteurs $3, 7, 1+2\sqrt{-5}, 1-2\sqrt{-5}$ n'est associé à un autre ou égal à une unité. Pour montrer que ces nombres sont tous primaires, observons que les normes correspondantes sont 9, 49, 21, 21. Si l'un des nombres correspondants est décomposable il faut que le corps contienne un entier à norme ± 3 ou ± 7. Chaque entier du corps a la forme $\alpha = a + b\sqrt{-5}$ (*voir* Chap. II, § 5), par conséquent $N(\alpha) = a^2 + 5b^2$ et cette expression ne peut pas prendre les valeurs $\pm 3, \pm 7$.

Il existe quand même de nombreux corps dans lesquels la décomposition en facteurs primaires est unique. Considérons par exemple le corps $K(\sqrt{-1})$; si η est un nombre arbitraire (non entier) on voit (par exemple par des considérations géométriques) qu'il existe un entier $\varkappa = k_1 + ik_2$ si rapproché de η que $N(\eta - \varkappa) \leqq \frac{1}{4}$. Soient alors α et β deux nombres entiers du corps $N(\alpha) \geqq N(\beta)$ et $\frac{\alpha}{\beta} = \varkappa + \rho'$ où $\varkappa$ est entier et $N(\rho') \leqq \frac{1}{4}$. On en tire

$$\alpha = \varkappa\beta + \rho, \tag{4}$$

où ρ est un entier et $N(\rho) < N(\beta)$. En appliquant le même procédé sur β et ρ, etc. on peut construire un algorithme d'Euclide, et de cet algorithme la démonstration de l'existence d'une décomposition unique en facteurs primaires se déduit comme dans la théorie ordinaire des nombres.

Ce procédé est applicable dans beaucoup de corps avec décomposition unique, par exemple les corps définis par

$$x^2 + x \pm 1 = 0, \qquad x^2 \pm 2 = 0, \qquad x^2 + x \pm 3 = 0.$$

L'existence d'un algorithme d'Euclide pour les normes est une condition suffisante, mais non nécessaire, pour une décomposition unique en facteurs primaires. On sait en effet, d'après *Dedekind*, que la décomposition dans le corps $K(\sqrt{-19})$ est unique, mais il n'existe pas un algorithme d'Euclide, c'est-à-dire, à deux entiers α et β du corps, $N(\alpha) \geqq N(\beta)$ on ne peut pas toujours trouver un entier $\varkappa$ tel que

$$N(\alpha - \varkappa\beta) < N(\beta).$$

Dedekind a montré, dans un Mémoire posthume, que la décomposition en éléments primaires est unique si l'on peut trouver un algorithme d'Euclide généralisé : A deux entiers α et β, β n'étant pas un diviseur de α, il existe toujours des entiers γ et δ tels que

$$0 < |N(\alpha\gamma - \beta\delta)| < |N(\beta)|, \qquad |N(\alpha)| \geqq |N(\beta)|.$$

Ce critère a été retrouvé récemment par *Hasse*, qui l'a déduit comme un cas spécial de recherches plus générales sur la décomposition en éléments primaires dans les domaines algébriques. On peut d'abord remplacer les normes dans ce critère par un caractère quelconque χ, qui ne prend que des valeurs entières, non négatives, telles que $\chi(\alpha\beta) = \chi(\alpha)\chi(\beta)$, $\chi(0) = 0$ et $\chi(\varepsilon) = 1$ pour les unités.

3. **Les idéaux.** — Pour les applications de la théorie des nombres algébriques, l'existence d'une décomposition unique en facteurs primaires est d'une importance fondamentale. Nous avons vu d'abord, que pour des corps arbitraires la décomposition n'est pas en général unique, et il est donc impératif de chercher un remplacement de ce théorème. C'était à la requête d'un tel substitut que *Kummer* introduisit premièrement la notion des *nombres idéaux* ou simplement les *idéaux*, la notion si féconde dans ses recherches ultérieures sur le problème de Fermat et les lois de réciprocité.

Les idéaux de Kummer étaient définis pour les corps circulaires seulement, c'est-à-dire pour les corps définis par des racines d'unité. La définition de Kummer est fondée sur des propriétés spéciales de ce corps et elle n'admet pas une généralisation directe aux corps arbitraires.

La théorie générale des idéaux pour un corps arbitraire fut créée par *Dedekind*, qui en publia le premier exposé dans ses suppléments à la deuxième édition de la « Théorie des nombres » de Dirichlet

(1871). Dans les éditions suivantes et dans des Mémoires nombreux il a considérablement augmenté et approfondi cette théorie. Entre les précurseurs de Dedekind il faut seulement mentionner *Selling*, qui a essayé de généraliser l'idée originale de Kummer plus directement que ne l'a fait Dedekind. Selling considère seulement les corps de Galois, c'est-à-dire les corps qui sont identiques à ses conjugués, mais sa théorie est en plusieurs manières très intéressante, quoique imparfaite et spéciale. L'espace ne me permet pas de présenter ici une discussion des théories ultérieures de Kronecker, Hensel, Prüfer, etc.

Dedekind définit un idéal comme il suit :

I. *Un idéal* A *est un système de nombres entiers du corps tel que :*

a. Si α *et* β *sont deux nombres de* A, $\alpha \pm \beta$ *le sera aussi;*

b. Si α *est un nombre de* A, *le produit* $\eta\alpha$, *où* η *est un entier arbitraire, est aussi contenu en* A.

Le nombre $0 = \alpha - \alpha$ est donc un élément de tout idéal. On peut aussi définir l'idéal d'une manière différente :

II. *Soient* $\alpha_1, \ldots, \alpha_r$, r *entiers arbitraires du corps; l'idéal* $A = [\alpha_1 \ldots \alpha_r]$ *est le système de nombres représentables dans la forme*

$$\alpha = \alpha_1\gamma_1 + \alpha_2\eta_2 + \ldots + \alpha_r\eta_r,$$

où les η_i *sont des entiers du corps.*

Nous allons démontrer l'équivalence des deux définitions I et II; adoptons pour le moment la définition I. Soit A un idéal; on peut alors montrer premièrement :

Il existe une base $\Omega_1 \ldots \Omega_n$ *de* A *telle que chaque nombre de* A *peut être représenté uniquement sous la forme*

$$\alpha = a_1\Omega_1 + \ldots + a_n\Omega_n, \tag{5}$$

où les a_i *sont des entiers rationnels.*

En effet, il existe dans A toujours des systèmes de n nombres linéairement indépendants, par exemple $\alpha\omega_1, \ldots, \alpha\omega_n$ où $\alpha \neq 0$ est un nombre de A et $\omega_1 \ldots \omega_n$ une base minimale du corps. Entre ces systèmes choisissons-en un pour lequel le discriminant a une valeur

absolue minimale. On déduit par les mêmes conclusions comme dans la démonstration de l'existence d'une base minimale du corps, que ce système est actuellement une base de l'idéal. On peut exprimer une base par toute autre avec des coefficients rationnels entiers et le déterminant ± 1. Le discriminant d'une base s'appelle parfois *discriminant de l'idéal.*

Si l'on adopte la définition I pour l'idéal tous les systèmes définis par II seront aussi des idéaux. A l'autre côté, tout idéal A d'après I est un idéal II avec la représentation

$$A = [\Omega_1, \ldots, \Omega_n],$$

où $\Omega_1 \ldots \Omega_n$ est une base. En effet, tout nombre de la forme

$$\alpha = \eta_1 \Omega_1 + \ldots + \eta_n \Omega_n,$$

est contenu en A d'après I, si les η_i sont des entiers du corps, et tout nombre de A est représentable dans cette forme même avec des coefficients rationnels.

4. Propriétés des idéaux. — Deux idéaux sont égaux s'ils contiennent les mêmes nombres; si l'on a

$$A = [\alpha_1, \ldots, \alpha_r] = [\alpha'_1, \ldots, \alpha'_{r'}] = A', \tag{6}$$

il faut et il suffit que les α_i soient contenus dans A' et que les α'_i soient contenus dans A, cela veut dire

$$\begin{cases} \alpha_i = \sum_{j=1}^{r'} \eta_j^{(i)} \alpha'_j & (i = 1, 2, \ldots, r), \\ \alpha'_i = \sum_{j=1}^{r} \mu_j^{(i)} \alpha_j & (i = 1, 2, \ldots, r'), \end{cases} \tag{7}$$

où les $\eta_j^{(i)}$ et $\mu_j^{(i)}$ sont des entiers du corps.

Ce critère nous donne des possibilités pour changer la représentation d'un idéal. On a par exemple

$$[\alpha_1, \alpha_2, \ldots, \alpha_r] = [\alpha_1 + \varkappa_2 \alpha_2 + \ldots + \varkappa_r \alpha_r, \alpha_2, \ldots, \alpha_r],$$
$$[\alpha_1, \alpha_2, \ldots, \alpha_r] = [\alpha_1, \alpha_2, \ldots, \alpha_r, \varkappa_1 \alpha_1 + \varkappa_2 \alpha_2 + \ldots + \varkappa_r \alpha_r],$$

où les $\varkappa_i$ sont des entiers. Considérons par exemple l'idéal

$$A = [9, 3 + 3\sqrt{-5}, -4 + 2\sqrt{-5}],$$

dans le corps $K(\sqrt{-5})$; il peut être réduit par la chaîne suivante :

$$A = [9, -6+3\sqrt{-5}, -4+2\sqrt{-5}] = [9, -6+3\sqrt{-5}, 2-\sqrt{-5}]$$
$$= [9, 2-\sqrt{-5}] = [2-\sqrt{-5}].$$

Nous allons montrer plus tard le théorème important : *Chaque idéal peut être réduit à l'une des deux formes*

$$A = [\alpha] \quad \text{ou} \quad A = [\alpha, \beta]. \tag{8}$$

On appelle *idéaux principaux* les idéaux de la forme $A = [\alpha]$; l'idéal principal A consiste de tous les nombres de la forme $\eta\alpha$ c'est-à-dire, de tous les multiples de α. *Deux idéaux principaux* $[\alpha]$ *et* $[\alpha']$ *sont égaux seulement si* α *et* α' *sont associés.* En effet, de (7) on obtient $\alpha = \eta\alpha'$, $\alpha' = \mu\alpha$, d'où $\eta\mu = 1$ et η et μ sont des unités. Cette condition est aussi suffisante.

Pour la comparaison de deux idéaux du second type (8) il existe le théorème suivant dû à *Hurwitz* [2] : *Il faut et il suffit pour que deux idéaux* $[\alpha, \beta]$ *et* $[\alpha', \beta']$ *soient égaux, qu'on puisse exprimer* α' *et* β' *par* α *et* β

$$\alpha' = \lambda\alpha + \mu\beta, \qquad \beta' = \nu\alpha + \rho\beta,$$

tel que $\lambda\rho - \mu\nu = 1$.

Entre les idéaux spéciaux d'un corps il faut mentionner l'idéal *zéro* qui consiste du nombre zéro seulement, et *l'idéal unité* $E = [1]$, qui consiste de tous les entiers du corps. Ces deux idéaux ont des propriétés spéciales et il est parfois commode de les exclure dans les considérations générales sur les idéaux. La base de E est une base minimale et son discriminant est le discriminant du corps.

Pour donner une illustration considérons les idéaux du corps rationnel. Un idéal

$$A = [a_1, \ldots, a_r]$$

consiste des nombres de la forme

$$a = x_1 a_1 + \ldots + x_r a_r,$$

où les x_i et a_i sont des entiers rationnels. Soit d le plus grand diviseur commun des a_i; d'après un théorème bien connu de la théorie élémentaire des nombres, on peut déterminer des $x_i^{(0)}$ tels que

$$d = x_1^{(0)} a_1 + \ldots + x_r^{(0)} a_r.$$

Le nombre d et tous les multiples de d sont donc contenus en A; à l'autre côté, tous les nombres de A sont évidemment divisibles par d et l'on a simplement $A = [d]$; *dans le corps rationnel tous les idéaux sont des idéaux principaux.*

Il existe un grand nombre de corps ayant la même propriété; par exemple, dans tous les corps quadratiques mentionnés à la fin du paragraphe 2 les idéaux sont tous principaux. Nous allons voir, que la décomposition en facteurs primaires dans tels corps est unique et leur théorie arithmétique ressemble donc fortement à la théorie ordinaire des nombres.

Les corps dans lesquels tous les idéaux sont principaux sont caractérisés par le critère de *Dedekind-Hasse* (*voir* § 2). *Il faut et il suffit, pour qu'un corps* K *ne contienne que des idéaux principaux, qu'il existe en* K *un algorithme d'Euclide généralisé : à deux entiers* α *et* β, $|N(\alpha) \geq |N(\beta)|$, α *n'étant pas divisible par* β, *il existe toujours deux entiers* γ *et* δ *tels que*

$$0 < |N(\alpha\gamma - \beta\delta)| < |N(\beta)|.$$

Ce critère, quoique intéressant au point de vue théorique, ne donne pas en général une méthode commode pour déterminer le caractère des idéaux et il faut ordinairement avoir recours à un calcul effectif du nombre des classes idéales du corps.

5. **Multiplication. Facteurs et diviseurs.** — Soient

$$A = [\alpha_1, \ldots, \alpha_r], \qquad A' = [\alpha'_1, \ldots, \alpha'_{r'}] \tag{9}$$

deux idéaux donnés, le système de nombres formés par tous les produits d'un nombre de A et un nombre de A′ et les sommes de tels produits forment, on le voit facilement, un idéal qu'on appelle *produit* de A et A′ dénoté par AA′. On peut représenter le produit dans la forme

$$C = AA' = [\alpha\alpha'_1, \ldots, \alpha_i\alpha'_j, \ldots, \alpha_r\alpha'_{r'}] \tag{10}$$

et cette représentation peut aussi servir de définition du produit. Il est facile de montrer, d'après (7), que l'idéal (10) est indépendant des représentations particulières choisies pour A et A′.

Pour les idéaux principaux, cette multiplication correspond à la multiplication ordinaire : de $A = [\alpha]$, $B = [\beta]$ on obtient

$AB = [\alpha\beta]$. L'idéal unité $E = [1]$ joue le rôle de l'unité de multiplication parce que $EA = A$ pour tout idéal A.

Nous dirons qu'un idéal A a le facteur idéal D si l'on peut trouver un idéal C tel que $A = DC$.

Il faut observer la propriété suivante des facteurs : *Si* D *est un facteur de* A, *tous les nombres de* A *sont contenus dans* D. Soient $D = [\delta_1, \ldots, \delta_t]$ et $C = [\gamma_1, \ldots \gamma_s]$ et par la définition de la multiplication

$$A = [\delta_1\gamma_1, \ldots, \delta_i\gamma_j, \ldots, \delta_t\gamma_s],$$

et chaque nombre de A a la forme

$$\alpha = \sum_{i,j} \eta_{ij}\,\delta_i\gamma_j = \sum_i \lambda_i\,\delta_i = \delta,$$

où δ est un nombre de D. Ce théorème, un peu surprenant au premier moment, s'explique facilement si l'on considère des idéaux spéciaux; par exemple, dans le corps rationnel l'idéal $[6]$ est divisible par $[2]$, et tous les nombres de la forme $6k$ sont aussi de la forme $2k_1$.

Nous dirons aussi qu'un idéal B est un *diviseur* de l'idéal A si tous les nombres de A sont contenus en B. Nous venons de montrer que chaque facteur de A est aussi un diviseur; le théorème inverse : *Chaque diviseur de* A *est aussi un facteur*, est beaucoup plus profond et la démonstration en est un des objets des recherches suivantes.

Si l'idéal principal $[\alpha]$ a le diviseur $[\delta]$, on aura $\alpha = \gamma\delta$ et δ est donc un diviseur de α dans le sens ordinaire.

Soient $A = [\alpha_1, \ldots, \alpha_r]$, $B = [\beta_1, \ldots, \beta_s]$ deux idéaux donnés; l'idéal composé

$$D = [\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s] \tag{11}$$

s'appelle *le plus grand diviseur commun de* A *et* B. Ce nom se justifie par les propriétés suivantes : 1° D *est un diviseur de* A *et de* B; D se compose en effet de tous les nombres de la forme $\alpha + \beta$, α étant un nombre de A et β un nombre de B, et pour $\beta = 0$ on obtient tous les nombres de A, c'est-à-dire, A est divisible par D et ainsi pour B; 2° *Tout diviseur commun* D′ *de* A *et* B *est un diviseur de* D. Tous les nombres de A et tous les nombres de B, par conséquent tous les nombres de D sont contenus en D′.

Cette définition montre qu'un idéal arbitraire $A = [\alpha_1, \ldots, \alpha_r]$ peut être considéré comme le plus grand diviseur commun des idéaux principaux $[\alpha_1], \ldots, [\alpha_r]$. Si l'idéal D en (11) est l'idéal unité, nous dirons que A *et* B *sont premiers entre eux*. Dans ce cas il existe donc un nombre α dans A et β dans B tel que

$$\alpha + \beta = 1 \tag{12}$$

et cette condition est aussi suffisante, parce que dans ce cas D doit contenir l'unité et par conséquent tous les entiers du corps. Cette définition nous donne aussi une manière de définir des *nombres* premiers entre eux. Deux entiers α_1 et α_2 sont premiers entre eux, si les idéaux principaux correspondants $[\alpha_1]$ et $[\alpha_2]$ sont premiers entre eux. De (12) le théorème suivant s'ensuit : *Si deux entiers* α_1 *et* α_2 *sont premiers entre eux, on peut trouver des entiers* λ *et* μ *du corps tels que*

$$\lambda\alpha_1 + \mu\alpha_2 = 1. \tag{13}$$

L'analogie avec le théorème ordinaire des nombres est évidente, ainsi que dans le théorème suivant : *Si le produit* BC *est divisible par* A, *et* A *et* B *sont premiers entre eux, alors* C *est divisible par* A. De (12) on obtient pour un nombre arbitraire γ de C

$$\gamma = \alpha\gamma + \beta\gamma.$$

Ici $\beta\gamma$ est un nombre de BC, par conséquent un nombre de A et γ est donc un nombre de A, c'est-à-dire tous les nombres de C sont contenus en A.

Nous montrerons enfin : *Un idéal donné* A *n'a qu'un nombre fini de diviseurs* (*ou facteurs*). Soit a un entier rationnel contenu en A, par exemple $a = N(\alpha)$, où α est un nombre de A. Chaque diviseur de A est aussi un diviseur de l'idéal $[a]$, et le théorème est donc une conséquence du lemme : *Un nombre rationnel a n'est contenu que dans un nombre fini d'idéaux.* Soit $\omega_1, \ldots, \omega_n$ une base minimale du corps; un entier arbitraire α peut être représenté sous la forme

$$\alpha = g_1\omega_1 + \ldots + g_n\omega_n.$$

Nous divisons les coefficients entiers g_i par a

$$g_i = q_i a + r_i, \qquad 0 \leqq r_i \leqq a - 1,$$

on a donc $\alpha = \lambda a + \rho$, où λ est entier et ρ est l'un des a^n nombres

$$\rho = r_1\omega_1 + \ldots + r_n\omega_n. \tag{14}$$

Soit d'abord a contenu dans l'idéal $[\alpha_1, \ldots, \alpha_r]$; nous représentons chaque α_i sous la forme $\alpha_i = \lambda_i a + \rho_i$, où ρ_i est un des nombres (14). On a donc pour A la réduction suivante (*voir* § 4) :

$$A = [\alpha_1, \ldots, \alpha_r, a] = [\lambda_1 a + \rho_1, \ldots, \lambda_r a + \rho_r, a] = [\rho_1, \ldots, \rho_r, a],$$

le nombre des ρ_i différents est fini, ce qui ne donne qu'un nombre fini de possibilités pour A. Si l'on introduit la notion des *congruences* (*voir* § 1, Chap. IV) en écrivant $\lambda \equiv \mu \pmod{A}$ si la différence $\lambda - \mu$ appartient à A, il s'ensuit de cette démonstration que chaque entier est congru à l'un des résidus (14).

6. **Idéaux premiers.** — Un idéal P est dit *premier s'il n'a pas de diviseurs;* il est évident qu'un idéal premier n'a pas de facteurs, l'inverse qu'un idéal sans facteurs est un idéal premier va suivre du théorème cherché sur l'identité de facteurs et diviseurs.

On peut aussi caractériser l'idéal premier dans une manière différente : Un idéal P est premier si le produit $\alpha\beta$ appartient à P seulement si α ou β est un élément de P. Un idéal premier P au sens antérieur à cette propriété; il s'ensuit même du paragraphe 5, qu'un produit AB de deux idéaux n'est divisible par P que si l'un des facteurs a le diviseur P. Pour montrer l'équivalence de la nouvelle définition avec la première, soit P un idéal avec la propriété indiquée et supposons qu'il a le diviseur propre P'; il y a alors en P' un élément α qui n'appartient pas à P. Les puissances α, α^2, ..., sont toutes en P'; dans le paragraphe 5 nous avons montré qu'il n'y a qu'un nombre fini d'entiers différents (mod P) et l'on aura donc $\alpha^a \equiv \alpha^b \pmod{P}$ pour quelques a et b différents; le nombre $\alpha^b(\alpha^{a-b} - 1)$ est en P et d'après la supposition on trouvera que $\alpha^{a-b} - 1$ est en P, par conséquent en P', c'est-à-dire -1 est en P' et P' est l'idéal unité.

7. **Le théorème fondamental.** — Le but principal de ce paragraphe est la démonstration du théorème fondamental de la théorie des idéaux :

Chaque idéal peut être représenté uniquement comme un produit d'un nombre fini d'idéaux premiers.

Nous commençons par montrer : *Chaque idéal est un diviseur d'un produit* $P_1 \dots P_s$ *d'idéaux premiers, où chaque* P_i *est un diviseur de* A. Ce théorème est évident pour un idéal premier. Soit donc $A = [\alpha_1, \dots, \alpha_r]$ un idéal non premier; il y a alors d'après le paragraphe 6 un produit $\beta\gamma$ en A, où β et γ n'appartiennent pas à A. Les idéaux

$$B = [\alpha_1, \dots, \alpha_r, \beta], \qquad C = [\alpha_1, \dots, \alpha_r, \gamma],$$

sont des diviseurs propres de A et leur produit BC aura le diviseur A. Si le théorème est vrai pour B et C il le sera aussi pour A; supposons donc qu'il n'est pas vrai pour B. Il y a encore un diviseur propre B' de B pour qui le théorème n'est pas valide, etc., ce qui donnera une infinité de diviseurs différents pour A.

Nous avons jusqu'à présent considéré seulement les idéaux formés par des entiers. Il est parfois commode d'introduire des *idéaux fractionnaires* contenant aussi des nombres non entiers. Dans ce but nous donnerons une définition un peu plus générale des idéaux.

Un idéal A est un système de nombres du corps tel que : 1° Si α et β sont éléments de A, les nombres de la forme $\alpha\lambda + \beta\mu$ où λ et μ sont entiers, le seront aussi; 2° il existe un nombre fixe τ tel que $\tau\alpha$ est entier pour chaque nombre α de A. Un idéal contenant seulement des entiers s'appelle *idéal entier*.

On voit comme auparavant qu'on peut représenter chaque idéal fractionnaire sous la forme $[\alpha_1, \dots, \alpha_r]$ et qu'il existe aussi une base $\omega_1, \dots, \omega_n$ de nombres en A tel que chaque nombre de l'idéal est représentable sous la forme

$$\alpha = \lambda_1\omega_1 + \dots + \lambda_n\omega_n$$

avec des coefficients entiers rationnels. On définit la multiplication des idéaux comme au paragraphe 5.

Soit P un idéal premier; la totalité des nombres α tel que $[\alpha]$ P est un idéal entier forment évidemment un idéal que nous allons dénoter par P^{-1}. *L'idéal* P^{-1} *n'est pas entier*. Soit en effet $\pi \neq 0$ un nombre arbitraire de P. L'idéal $[\pi]$ est un diviseur d'un produit $P_1 \dots P_r$ d'idéaux premiers (§ 6); nous supposons que le nombre de facteurs est choisi minimal. L'idéal $[\pi]$ est divisible par P et l'un des facteurs P_i est donc égal à P (§ 5); soit $P_1 = P$. Le produit $P_2 \dots P_r$ n'est pas divisible par $[\pi]$ parce qu'il contient moins que r facteurs; il contient

par conséquent un nombre γ qui n'est pas en $[\pi]$ et $\gamma_1 = \gamma\pi^{-1}$ sera fractionnaire. Le produit $[\gamma]P$ est un idéal entier divisible par $[\pi]$ et $[\gamma_1]P$ sera un idéal entier, c'est-à-dire γ_1 est un élément de P^{-1}.

Nous allons montrer que $A = PP^{-1}$ est l'idéal unité E. On voit que A est un idéal entier et parce que P^{-1} doit contenir l'unité, A sera un diviseur de P, par conséquent $A = E$ ou $A = P$. Dans le dernier cas soit $\omega_1, \ldots, \omega_n$ une base de P et γ un nombre fractionnaire de P^{-1}. Les produits $\gamma\omega_i$ sont tous en P et par suite représentables dans la forme

$$\gamma\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j$$

avec des coefficients entiers rationnels; γ serait alors entier contre notre hypothèse (*voir* § 1, Chap. II).

Ces résultats nous donnent : Chaque idéal est un produit d'idéaux premiers. Soit, en effet, A un idéal diviseur du produit $P_1 P_2 \ldots P_r$ d'idéaux premiers, où chaque P_i est un diviseur de A. Supposons r minimal, et encore que le théorème a été montré pour chaque idéal divisant un produit d'un nombre moins de facteurs. En multipliant par P_1^{-1}, on obtient que $P_2 \ldots P_r$ sera divisible par l'idéal entier AP_1^{-1}, et le théorème est donc vrai pour AP_1^{-1}, d'où l'on déduit aussitôt la validité pour A.

La démonstration du théorème fondamental s'achève en montrant que la représentation comme produit d'idéaux premiers est unique. C'est évidemment une conséquence du résultat suivant : *Si l'idéal* $A = P_1 \ldots P_r$ *est divisible par* $B = Q_1 \ldots Q_s$ *chaque idéal premier* Q *apparaît entre les* P *au moins autant de fois qu'en la représentation de* B. Il s'ensuit déjà du paragraphe 6, que chaque facteur premier Q apparaît entre les P et si A le contient a fois; B, b fois, où $b > a$ on trouvera que l'idéal $A(Q^{-1})^a$ est divisible par $B(Q^{-1})^a$, quoique le premier n'a pas le diviseur Q.

Cette démonstration du théorème fondamental est fondée sur l'idée d'une démonstration de Krull et v. d. Waerden; je l'ai préféré ici aux démonstrations classiques parce qu'elle s'applique non seulement aux entiers algébriques, mais aussi, avec des modifications légères, aux domaines beaucoup plus généraux.

Entre les conséquences du théorème fondamental est le résultat déjà signalé : *Chaque diviseur* B *d'un idéal* A *est aussi un facteur*

de A. Soit

$$A = P_1^{e_1} \dots P_r^{e_r},\ B = P_1^{f_1} \dots P_r^{f_r},\ e_i \geqq 0,\ f_i \geqq 0,\ (i = 1, 2, \dots, r);$$

nous avons vu que $e_i \geqq f_i$ pour tous i et l'on aura donc $A = BC$ si $C = P_1^{e_1 - f_1} \dots P_r^{e_r - f_r}$.

A chaque idéal A *il existe un idéal* B *tel que le produit* $AB = [c]$ *est un idéal principal.* Soit $[c]$ un nombre arbitraire de A; l'idéal $[c]$ a le diviseur A, d'où le théorème s'ensuit. Ce dernier théorème est le lemme central de la démonstration classique du théorème fondamental par Hurwitz [3]. On en tire sans difficultés l'identité de diviseurs et facteurs, et aussi le fait que de $AB = AC$ suivra $B = C$, donnant immédiatement le théorème fondamental.

Hurwitz déduit ce théorème à l'aide du théorème de Kronecker :

Soient

$$f(x) = \alpha_0 x^n + \dots + \alpha_{n-1} x + \alpha_n,$$
$$g(x) = \beta_0 x^m + \dots + \beta_{m-1} x + \beta_m$$

deux polynomes avec coefficients entiers et algébriques, et soit

$$f(x) g(x) = \gamma_0 x^{n+m} + \dots + \gamma_{n+m-1} x + \gamma_{n+m}.$$

S'il existe un entier algébrique ν *qui divise tous les coefficients* γ_i *du produit, ce nombre est aussi un diviseur de tous les produits* $\alpha_i \beta_j (i = 1, 2, \dots, n; j = 0, 1, \dots, m)$.

Il y a pour ce théorème outre les démonstrations de Kronecker, d'autres par Dedekind, Hurwitz, Mertens et Steinitz (*voir* ma note au Mémoire de Dedekind, *Œuvres complètes*, t. II, p. 39).

Il y a aussi des démonstrations du théorème $AB = [c]$ qui ne dépendent pas du théorème de Kronecker. Je fais mention ici de la déduction de Hilbert appliquant la théorie des corps de Galois, et la démonstration de Furtwangler [2] fondée sur les propriétés des formes décomposables et leurs classes. Furtwangler [3] a déduit les théorèmes fondamentaux de la théorie des idéaux aussi dans une manière différente en employant une représentation des idéaux par des grillages de points dans un espace à n dimensions. Cette idée a été utilisée premièrement par Klein dans la théorie des corps quadratiques, et elle est aussi étroitement liée avec les recherches de Minkowski sur le même sujet. Il faut mentionner finalement la

démonstration nouvelle très originale de notre théorème donnée plus tard par Hurwitz [3], [4]. Hurwitz introduit une généralisation de l'algorithme d'Euclide d'où l'on trouve que le nombre des classes des idéaux est fini, ce qui montrera à son tour le théorème.

8. Applications du théorème fondamental; idéaux fractionnaires. — Nous avons vu que tout idéal A possède une décomposition unique

$$A = P_1^{a_1} \dots P_r^{a_r} \tag{15}$$

en facteurs premiers. La décomposition d'un entier α en facteurs premiers est la décomposition

$$[\alpha] = P_1^{e_1} \dots P_r^{e_r}$$

de l'idéal principal correspondant, très souvent on ne fait aucune distinction entre un nombre et l'idéal correspondant.

Soient d'abord

$$[\alpha] = P_1^{e_1} \dots P_r^{e_r}, \qquad [\beta] = P_1^{f_1} \dots P_r^{f_r} \tag{16}$$

la décomposition de deux idéaux principaux; l'idéal $A = [\alpha, \beta]$ est alors, d'après le paragraphe 7, le plus grand diviseur commun de $[\alpha]$ et $[\beta]$. Mais on peut aussi déduire ce diviseur commun directement de (16), et l'on obtient donc pour A une représentation (15) où les exposants a_i pour chaque i sont les plus petits des nombres e_i et f_i en (16). On peut généraliser cette remarque à un idéal arbitraire $A = [\alpha_1, \dots, \alpha_r]$, ce qui donnera un point de vue nouveau pour ce symbole.

Nous avons montré l'existence d'une décomposition en idéaux premiers pour chaque idéal, mais on voit aussi que notre démonstration ne donne aucune méthode pour déterminer effectivement cette décomposition. Il suffit évidemment de trouver la décomposition de tous les idéaux principaux ou même les idéaux principaux rationnels, ce qui réduit notre problème à la proposition suivante : *Trouver la décomposition en idéaux premiers de tous les nombres premiers rationnels.* C'est alors un des problèmes les plus importants de la théorie des idéaux.

La notion des idéaux fractionnaires nous permet de définir en général le quotient de deux idéaux : le quotient $C = \frac{A}{B}$ est un idéal

tel que $BC = A$. Pour établir l'existence du quotient, choisissons B' tel que $BB' = [b]$; alors on obtient

$$C = \frac{AB'}{[b]},$$

c'est-à dire, C est le système des nombres de AB' divisés par b. Le quotient est unique, parce que de $CB = A = C_1 B$ on obient $C = C_1$. Si E est l'idéal unité et A un idéal arbitraire, on a

$$\frac{A}{E} = A, \qquad \frac{A}{A} = E,$$

ce qui s'ensuit de $AE = A$. On voit donc : *Les idéaux fractionnaires du corps forment un groupe.*

De la définition du quotient on tire

$$\frac{AD}{BD} = \frac{A}{B};$$

on peut donc abréger les quotients dans la manière ordinaire. Cette remarque nous donne encore : *Chaque idéal fractionnaire peut être représenté uniquement comme le quotient de deux idéaux entiers et premiers entre eux.* Ce théorème s'applique particulièrement à des idéaux principaux $[\eta]$ formés par un nombre arbitraire non entier du corps.

Définissons enfin la *divisibilité* des idéaux fractionnaires. On dit que A est divisible par B si $A = CB$ où C est un idéal *entier*. Un idéal principal $[\eta]$ est donc divisible par B si $[\eta] = BC$, où C est entier; on voit comme plus haut, que les nombres de BC sont tous contenus en B et il s'ensuit que η est un nombre de B. Réciproquement, soit η un nombre de B, et soit τ un nombre tel que $[\tau]B = B'$ est un idéal entier; alors $\eta\tau$ est un élément de B', c'est-à-dire $[\tau][\eta] = CB'$ d'où l'on tire $[\eta] = CB$, où C est entier. Il résulte donc : *Un nombre η est contenu dans l'idéal* B *seulement dans le cas où* $[\eta]$ *est divisible par* B. Déterminons comme une application tous les idéaux contenant l'unité. Alors $[1] = E = CB$, où C est entier, d'où

$$B = \frac{1}{C}.$$

L'unité est contenue seulement dans les idéaux qui sont égaux au réciproque d'un idéal entier.

CHAPITRE IV.

1. Congruences pour des modules idéaux. — Soit A un idéal entier, et soient α et β deux entiers du corps. Nous écrivons comme auparavant

$$\alpha \equiv \beta \pmod{A}, \tag{1}$$

si la différence $\alpha - \beta$ est un nombre de A. Une congruence $\alpha \equiv 0 \pmod{A}$ signifie alors que α est un nombre de A, ou bien que α est divisible par A. Si $A = [\varkappa]$ est un idéal principal, on obtient de (1) $\alpha - \beta = \rho\varkappa$, c'est-à-dire la différence $\alpha - \beta$ est divisible par $\varkappa$, ce qu'on peut aussi exprimer par la congruence équivalente

$$\alpha \equiv \beta \pmod{\varkappa}.$$

Les congruences pour des modules idéaux sont donc une généralisation naturelle des congruences ordinaires de la théorie des nombres. Ils ont aussi des propriétés simples rappelant celles des congruences ordinaires.

De $\alpha \equiv \beta, \beta \equiv \gamma \pmod{A}$ on conclut $\alpha \equiv \gamma$. De $\alpha \equiv \beta, \gamma \equiv \delta \pmod{A}$, on conclut

$$\alpha \pm \gamma \equiv \beta \pm \delta \pmod{A},$$
$$\alpha\gamma \equiv \beta\delta \pmod{A}.$$

Toute congruence $\pmod{A}$ est aussi vraie pour le module D, où D est un diviseur de A. On peut aussi diviser des congruences sous les conditions suivantes : De

$$\alpha\gamma \equiv \beta\gamma \pmod{A}, \tag{2}$$

on tire

$$\alpha \equiv \beta \left(\mod \frac{A}{D}\right), \tag{3}$$

où D est le plus grand diviseur commun de A et de γ (c'est-à-dire de $[\gamma]$). Soit en effet $[\gamma] = D\Gamma$, $A = DA'$; d'après (2) l'idéal $[\alpha - \beta][\gamma]$ est divisible par A, d'où l'on voit que $[\alpha - \beta]$ est divisible par A', ce qu'on peut exprimer par (3).

Entre les théorèmes importants sur les congruences je fais mention

premièrement du suivant : *Une congruence linéaire*

$$\alpha x \equiv \beta \pmod{A} \tag{4}$$

où α *et* A *sont premiers entre eux admet toujours une solution unique.* Pour le montrer, observons que le plus grand diviseur commun de $[\alpha]$ et A est l'idéal unité, et que chaque entier β du corps aura par suite une représentation comme la somme d'un nombre η de A et $\alpha\varkappa$ de $[\alpha]$ (*voir* § 7, Chap. III). De cette représentation $\beta = \varkappa\alpha + \eta$ on tire immédiatement la solution $x \equiv \varkappa \pmod{A}$ de (4). Cette solution est unique, parce que de $\alpha\varkappa \equiv \beta \equiv \alpha\varkappa_1$ on tirera $\alpha(\varkappa_1 - \varkappa) \equiv 0$ ou bien $\varkappa_1 \equiv \varkappa \pmod{A}$.

Dans le cas où α et A possèdent le facteur commun D, la congruence (4) n'a pas de solution si $\beta \not\equiv 0 \pmod{D}$. Si la condition $\beta \equiv 0 \pmod{D}$ est satisfaite, β appartient au plus grand diviseur commun de $[\alpha]$ et $[A]$ et l'on peut représenter β comme une somme d'un nombre de $[\alpha]$ et d'un nombre de A, ce qui donnera comme plus haut une solution de (4).

Le théorème suivant est utile dans des applications nombreuses : *Soient* $\lambda_1, \lambda_2, \ldots, \lambda_r$ *des entiers arbitraires, et* $A_1, \ldots, A_r$, r *idéaux tous premiers entre eux. Alors il existe toujours une solution des congruences simultanées*

$$x \equiv \lambda_1 \pmod{A_1}, \quad \ldots, \quad x \equiv \lambda_r \pmod{A_r}. \tag{5}$$

Pour trouver explicitement une solution de (5) posons

$$A = A_1 \ldots A_r, \qquad B_i = \frac{A}{A_i} \qquad (i = 1, 2, \ldots, r).$$

Alors A_i et B_i sont premiers entre eux et l'on a $\alpha_i + \beta_i = 1$, où α_i et β_i sont des nombres de A_i et B_i choisis convenablement. Les nombres β_i satisfont donc aux congruences

$$\beta_i \equiv 1 \pmod{A_i}, \qquad \beta_i \equiv 0 \pmod{A_j},\ i \neq j), \tag{6}$$

d'où l'on tire facilement que

$$x \equiv \lambda_1\beta_1 + \lambda_2\beta_2 + \ldots + \lambda_r\beta_r \pmod{A} \tag{7}$$

est une solution de (5). On montrera d'abord aussi, que la solution (7) de (5) est unique (mod A).

Ce théorème nous permet de déduire une conséquence importante :

Soient $P_1, P_2, \ldots, P_r$ *un nombre d'idéaux premiers et soient* $a_1 \geqq 0, a_2 \geqq 0, \ldots, a_r \geqq 0$ *des nombres entiers rationnels donnés. Alors il existe un entier* γ *du corps divisible exactement par les puissances* $P_i^{a_i}$ $(i = 1, 2, \ldots, r)$ *de ces idéaux premiers*, c'est-à-dire, pour tout i, $[\gamma]$ est divisible par $P_i^{a_i}$ mais non par $P_i^{a_i+1}$.

Pour le montrer, soit P un idéal premier quelconque; alors il existe toujours un nombre premier π par rapport à P, savoir un nombre π divisible par P, mais non par P^2. En effet, au cas contraire tous les nombres de P seraient contenus en P^2, ce qui donnerait $P^2 = P$ et P serait l'idéal unité.

Soient donc $\pi_1, \pi_2, \ldots, \pi_r$ des nombres premiers par rapport à $P_1, P_2, \ldots, P_r$; les nombres $\pi_1^{a_1}, \pi_2^{a_2}, \ldots$ sont alors divisibles exactement par $P_1^{a_1}, P_2^{a_2}, \ldots$ et il existe d'après le théorème précédent un nombre γ tel que

$$\gamma \equiv \pi_i^{a_i} \pmod{P_i^{a_i+1}} \qquad (i = 1, 2, \ldots, r).$$

On voit sans difficulté que ce nombre a les propriétés désirées.

Nous déduirons enfin le théorème déjà énoncé au paragraphe 4 (Chap. III) : *Tout idéal* A *peut être représenté comme le plus grand diviseur commun de deux idéaux principaux*

$$A = [\alpha, \beta]. \tag{8}$$

Soit

$$A = P_1^{a_1} \ldots P_r^{a_r}$$

la décomposition de A en facteurs premiers; le nombre α en (8) peut être choisi arbitrairement dans A; soit

$$[\alpha] = P_1^{b_1} \ldots P_r^{b_r} Q,$$

où $b_i \geqq a_i$ $(i = 1, 2, \ldots, r)$ et Q n'est divisible par aucun des P_i. D'après le théorème que nous venons de déduire il existe un nombre β de A divisible exactement par $P_1^{a_1}, \ldots, P_r^{a_r}$ et qui n'est divisible par aucun des facteurs premiers de Q; le plus grand diviseur commun de $[\alpha]$ et $[\beta]$ est donc A.

2. Les normes des idéaux. — Soit A un idéal entier; si $\alpha \equiv \beta \pmod{A}$, nous dirons que les entiers α et β appartiennent à la même *classe résiduaire* (mod A). *Le nombre de ces classes est fini.* Ce résultat fut déjà déduit dans la démonstration du théorème fonda-

mental (*voir* § 5, Chap. III, *fin*); les mêmes considérations montrent qu'on aura pour un idéal principal $[a]$, a rationnel, et un entier arbitraire α une congruence de la forme

$$\alpha \equiv r_1\omega_1 + \ldots + r_n\omega_n \pmod{[a]}, \tag{9}$$

où $0 \leqq r_i \leqq a-1$ et $\omega_1, \ldots, \omega_n$ est une base minimale, ce qui fait voir que le nombre des classes $(\mathrm{mod}[a])$ est au plus égal à a^n. C'est en effet le nombre exact des classes, parce que les a^n nombres (9) sont tous différents $(\mathrm{mod}[a])$ d'une congruence

$$r_1\omega_1 + \ldots + r_n\omega_n \equiv r'_1\omega_1 + \ldots + r'_n\omega_n \pmod{[a]},$$

l'on tire que le nombre

$$\frac{r_1 - r'_1}{a}\omega_1 + \ldots + \frac{r_n - r'_n}{a}\omega_n$$

est entier, quoique les coefficients ne sont pas tous entiers ce qui est incompatible avec les propriétés d'une base minimale.

Le nombre NA des classes (modA) s'appelle *norme* de l'idéal A. On a donc $\mathrm{N}[a] = |a|^n$, si a est un entier rationnel. Nous allons montrer comment on peut en général déterminer la norme d'un idéal; dans la suite nous traiterons aussi le problème plus profond d'établir un *système résiduaire* (modA), c'est-à-dire un système de NA nombres

$$\rho_1, \rho_2, \ldots, \rho_{\mathrm{NA}}, \tag{10}$$

tel que chaque nombre du corps est congru à un seul des nombres (modA).

Pour le corps rationnel ces problèmes sont triviaux. Il y a m classes résiduaires $(\mathrm{mod}\,m)$ et un système résiduaire complet est donné par les nombres $0, 1, \ldots, m-1$.

La norme d'un idéal est d'après la définition un entier rationnel positif. *On a* $\mathrm{NA} = 1$ *seulement pour l'idéal unité.* Si $\mathrm{NA} = 1$ tous les entiers appartiennent à la même classe (modA), par exemple

$$\omega \equiv 0 \pmod{\mathrm{A}}$$

pour chaque entier ω du corps, et A contient tous les entiers.

Dans un système résiduaire complet (10) (modA), on aura

$$\rho_i \not\equiv \rho_j \pmod{\mathrm{A}} \quad (\text{pour } i \neq j)$$

et NA nombres ayant cette propriété constituent un système résiduaire complet. Il est donc évident que les nombres

$$\rho_1+1,\quad \rho_2+1,\quad \ldots,\quad \rho_{NA}+1 \tag{11}$$

forment aussi un système résiduaire pour le même idéal et chaque nombre de (11) est congru à un seul nombre de (10) et réciproquement. On aura alors

$$\rho_1+\ldots+\rho_{NA}\equiv(\rho_1+1)+\ldots+(\rho_{NA}+1)\qquad(\mathrm{mod}\,A),$$

d'où $NA\equiv 0\ (\mathrm{mod}\,A)$. *La norme d'un idéal appartient à l'idéal.* On en tire aussi : *Il n'y a qu'un nombre fini d'idéaux à norme donnée.* En effet si la norme $N=NA$ est donnée, N est contenu dans les idéaux A possibles et nous avons montré au paragraphe 7 (Chap. III), qu'il n'ya qu'un nombre fini d'idéaux contenant un entier rationnel donné.

Le théorème fondamental sur les normes des idéaux est le suivant : *La norme d'un produit est le produit des normes des facteurs* $N(AB)=NA.NB$.

Pour le montrer, soient

$$\alpha_1,\quad \alpha_2,\quad \ldots,\quad \alpha_{NA};\qquad \beta_1,\quad \beta_2,\quad \ldots,\quad \beta_{NB}$$

deux systèmes résiduaires pour A et pour B. On construit alors un système résiduaire (mod AB) comme il suit : D'après le paragraphe 1 il existe un nombre ρ en B tel que le plus grand diviseur commun de $[\rho]$ et AB est B; j'affirme que les NA.NB nombres

$$\rho\alpha_i+\beta_j\qquad(i=1,2,\ldots,NA,\ j=1,2,\ldots,NB) \tag{12}$$

forment un système résiduaire complet (mod AB), ce qui rend évident notre théorème. Il faut donc montrer que les nombres (12) sont tous différents (mod AB) et que chaque entier est congru à l'un de ces nombres. Si

$$\rho\alpha_{i_1}+\beta_{j_1}\equiv\rho\alpha_i+\beta_j\qquad(\mathrm{mod}\,AB),$$

on aura $\beta_{j_1}\equiv\beta_j\ (\mathrm{mod}\,B)$ et par conséquent $j_1=j$ d'où l'on tire $\rho(\alpha_{i_1}-\alpha_i)\equiv 0\ (\mathrm{mod}\,AB)$, ce qui donne $\alpha_{i_1}\equiv\alpha_i\ (\mathrm{mod}\,A)$ et $i_1=i$. Pour montrer la seconde partie observons que $\omega\equiv\beta_i\ (\mathrm{mod}\,B)$ pour un entier arbitraire ω; posons $\omega=\beta_j+\lambda$ où $\lambda\equiv 0\ (\mathrm{mod}\,B)$. La congruence $x\rho\equiv\lambda\ (\mathrm{mod}\,AB)$ a donc une solution μ (*voir* § 1), ce qui

donne $\omega \equiv \beta_j + \mu\rho \pmod{AB}$ et si l'on écrit enfin $\mu = \alpha_l + \nu$ où $\nu \equiv 0 \pmod{A}$ on voit que ω est congru à l'un des nombres (12).

C. Q. F. D.

D'après ce théorème, on peut déterminer la norme d'un idéal A si l'on connaît les normes des idéaux premiers divisant A, et si $A = P_1 \dots P_t$ est la décomposition de A en idéaux premiers, on a $NA = NP_1 \dots NP_t$.

Soit d'abord P un idéal premier, il y a dans P des entiers rationnels, par exemple la norme de P; le plus petit de ces nombres rationnels est nécessairement un nombre premier p, parce que si $p = ab$, l'idéal P était aussi un diviseur de a ou de b. *Il faut et il suffit pour qu'un nombre rationnel a soit divisible par* P, *que a soit divisible par p*. Si a n'est pas divisible par p on peut écrire $a = qp + r$, $|r| < p$ et r est aussi divisible par P contre la propriété minimale de p.

Chaque idéal premier correspond donc, dans une manière unique, un nombre premier rationnel qu'il divise. Soit

$$[p] = P_1^{e_1} \dots P_r^{e_r} \tag{13}$$

la décomposition d'un nombre premier en facteurs premiers. On appelle l'*ordre* de P_l l'exposant e_l de P_l dans cette décomposition. On obtient de (13) en prenant la norme des deux côtés

$$p^n = (NP_1)^{e_1} \dots (NP_r)^{e_r}, \tag{14}$$

ce qui montre que la norme d'un idéal P_l est une puissance de p, $NP_l = p^{f_l}$, où f_l est appelé le *degré* de P_l. De (14) on déduit en comparant les exposants de p

$$n = e_1 f_1 + \dots + e_r f_l,$$

ce qui donne une connexion importante entre les ordres et les degrés des idéaux premiers divisant un nombre premier donné. La détermination effective des nombres e_l et f_l est identique au problème de la détermination de la décomposition des nombres premiers en idéaux premiers.

3. **Propriétés des normes.** — Nous avons déjà observé l'existence d'une base minimale pour un idéal quelconque A (§ 3, Chap. III); on

peut exécuter la construction d'une telle base dans la manière suivante : soit $\omega_1, \ldots, \omega_n$ une base minimale du corps. Pour chaque r, $1 \leqq r \leqq n$ il existe nombres de A représentables sous la forme

$$\alpha_r = a_{r,1}\omega_1 + \ldots + a_{r,r}\omega_r, \tag{15}$$

avec des coefficients entiers et $a_{r,r} > 0$, un tel nombre est par exemple $NA.\omega_r$. Nous choisissons à présent $a_{r,r}$ minimal pour chaque r et nous allons montrer que les nombres correspondants $\alpha_1, \ldots, \alpha_n$ forment une base de A. Les α_i sont tous contenus en A d'après définition, et le discriminant est

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = (a_{11}a_{22}\ldots a_{n,n})^2 \Delta(\omega_1, \ldots, \omega_n). \tag{16}$$

Il reste donc à montrer que tous les nombres de A sont exprimables par les α_i avec des coefficients entiers. Soit

$$\alpha = b_1\omega_1 + \ldots + b_n\omega_n$$

un nombre arbitraire de A; on déduit immédiatement de la propriété minimale de $a_{n,n}$ que b_n est divisible par $a_{n,n}$ (*voir* § 5, Chap. II), alors $b_n = k_n a_{n,n}$ et par conséquent

$$\alpha - k_n\alpha_n = b'_1\omega_1 + \ldots + b'_{n-1}\omega_{n-1}.$$

Ici b'_{n-1} est divisible par $a_{n-1,n-1}$, $b'_{n-1} = k_{n-1}a_{n-1,n-1}$ et l'on trouve de proche en proche la représentation cherchée.

D'une base de A de la forme (15) on déduit aussitôt la norme de A; on a en effet

$$NA = a_{1,1}a_{2,2}\ldots a_{n,n}. \tag{17}$$

La démonstration s'accomplit en montrant que les nombres

$$c_1\omega_1 + c_2\omega_2 + \ldots + c_n\omega_n \qquad (0 \leqq c_r \leqq a_{r,r} - 1) \tag{18}$$

forment un système résiduaire complet (mod A). Il est nécessaire de montrer que les nombres (18) sont tous différents (mod A) et que chaque entier est congru à l'un de ces nombres. Si deux nombres (18) sont égaux (mod A), on aura

$$(c_1 - c'_1)\omega_1 + \ldots + (c_n - c'_n)\omega_n \equiv 0 \pmod{A},$$

et il s'ensuit comme auparavant que $c_n - c'_n$ est divisible par $a_{n,n}$, c'est

à-dire $c_n = c'_n$; dans la même manière on établit l'identité de tous les coefficients c_r et c'_r. Pour montrer la seconde partie, soit

$$\omega = d_1\omega_1 + \ldots + d_n\omega_n$$

un entier arbitraire du corps; on voit sans difficulté qu'en soustrayant des multiples convenables des α_r (15) de ω on peut faire les coefficients du nombre résultant plus petits que $a_{r,r}$ $(r = 1, 2, \ldots, n)$ et ω est donc congru à un nombre (18).

De (18) et (16) on conclut

$$\Delta(\alpha_1, \ldots, \alpha_n) = \mathrm{NA}^2\Delta(\omega_1, \ldots, \omega_n), \tag{19}$$

et en observant que toutes les bases d'un idéal ont le même discriminant, on en tire le théorème : *Le discriminant d'un idéal* A *est égal à* $\mathrm{NA}^2.d$, *où d est le discriminant du corps*. On peut aussi exprimer ce résultat dans une manière un peu différente. Soit $\alpha_1, \ldots, \alpha_n$ une base arbitraire de l'idéal et soit

$$\alpha_i = a_{i,1}\omega_1 + \ldots + a_{i,n}\omega_n \qquad (i = 1, 2, \ldots, n) \tag{20}$$

la représentation des α_i par une base minimale du corps. Alors on a (*voir* § 4, Chap. II) : *Le déterminant* $|a_{ij}|$ *du système* (20) *est égal à* $\pm\,\mathrm{NA}$.

L'identité (19), valide pour une base arbitraire de l'idéal, nous permet de déduire encore une propriété importante des normes. Nous avons considéré jusqu'ici deux notions différentes des normes : La norme d'un nombre du corps (§ 4, Chap. II) et la norme d'un idéal. Nous sommes à présent en position de montrer que pour des idéaux principaux les deux notions sont identiques : pour un idéal principal $[\alpha]$, on a

$$\mathrm{N}[\alpha] = |\mathrm{N}(\alpha)|. \tag{21}$$

Il faut observer que la valeur absolue est nécessaire, la norme d'un idéal étant toujours positive, ce qui n'est pas en général vrai pour la norme d'un nombre. Les nombres de $[\alpha]$ sont tous de la forme $\alpha\omega$ et

$$\alpha\omega_1, \quad \ldots \quad \alpha\omega_n$$

est donc une base de l'idéal. Le discriminant de cette base est $\mathrm{N}(\alpha)^2 d$ et la comparaison avec (19) nous donne (21).

Les considérations suivantes rendront aussi plus clair la relation

entre les deux types de normes. Jusqu'à présent nous avons considéré un corps $K(\vartheta)$ ayant les corps conjugués $K(\vartheta^{(2)}), \ldots, K(\vartheta^{(n)})$, nous allons introduire pour le moment aussi le corps de Galois $\overline{K} = K(\vartheta^{(1)}, \ldots, \vartheta^{(n)})$ contenant toutes les fonctions rationnelles des $\vartheta^{(i)}$ avec des coefficients rationnels. A chaque idéal

$$A = [\alpha_1, \ldots, \alpha_r]$$

de K se composant des nombres $\alpha_1\lambda_1 + \ldots + \alpha_r\lambda_r$ (λ_i entiers de K) il correspond uniquement un idéal $\overline{A} = [\alpha_1, \ldots, \alpha_r]$ de $\overline{K}$ contenant les nombres $\alpha_1\bar{\lambda}_1 + \ldots + \alpha_r\bar{\lambda}_r$ ($\bar{\lambda}_i$ entiers de $\overline{K}$). Le corps $\overline{K}$ contient aussi tous les idéaux conjugués $\overline{A}_i = [\alpha_1^{(i)}, \ldots, \alpha_r^{(i)}]$ de $\overline{A}$. On peut alors montrer

$$\overline{A}_1\overline{A}_2 \ldots \overline{A}_n = [NA]. \tag{22}$$

Dans la démonstration suivante j'évite l'application des formes indéterminées ordinairement introduites pour la déduction de ce théorème. Il est d'abord évident que l'idéal $\overline{A}$ est indépendant de la représentation choisie pour l'idéal A. Nous trouvons une représentation commode de A par le lemme suivant : *On peut toujours représenter un idéal* A *dans la forme* $A = [\alpha, \beta]$ *tel que* $NA = [N(\alpha), N(\beta)]$. Soit α un nombre arbitraire de A et

$$A = P_1^{a_1} \ldots P_r^{a_r}, \qquad [\alpha] = P_1^{b_1} \ldots P_r^{b_r} Q_1^{c_1} \ldots Q_s^{c_s}$$

la décomposition en facteurs premiers de ces idéaux. D'après le paragraphe 1, on peut déterminer β en A tel que

$$[\beta] = P_1^{a_1} \ldots P_r^{a_r} R_1^{d_1} \ldots R_t^{d_t},$$

où les idéaux premiers R_i ne divisent aucun des nombres premiers rationnels divisibles par les P_i ou les Q_i. Les normes des R_i sont donc premières aux normes des P_i et Q_i d'où l'on tire l'exactitude de notre lemme.

Le nombre α étant arbitraire dans cette représentation, choisissons $\alpha = NA$, ce qui donne $A = [NA, \beta]$ et

$$\overline{A}_1 \ldots \overline{A}_n = [NA^n, \ldots, N(\beta)],$$

où tous les termes sauf le dernier contiennent un facteur NA. Le produit est donc divisible par NA et puisque $NA = [NA^n, N(\beta)]$ le produit contient le nombre NA, ce qui complètera la démonstration

de (22). Pour des démonstrations différentes voir par exemple Bauer.

Je fais mention finalement du fait que la notion de la norme peut aussi être généralisée aux idéaux fractionnaires. On définit

$$N\left(\frac{A}{B}\right) = \frac{NA}{NB},$$

et il n'est pas très difficile à montrer que la plupart des propriétés des normes se transfèrent aux idéaux fractionnaires, particulièrement les propriétés exprimées par les équations (19), (21) et (22).

4. **Les classes résiduaires premières.** — Soit α un entier arbitraire, s'il existe un facteur idéal commun D de α et l'idéal A, tous les nombres congrus à α (mod A) sont aussi divisibles par D, et si α est premier à A, tous les nombres congrus à α (mod A) sont premiers à A. Une classe résiduaire (mod A) qui ne contient que des nombres premiers à A, s'appelle *classe première* (mod A). On voit facilement, comme dans le cas rationnel, que les classes premières (mod A) forment un groupe par rapport à multiplication. Soit $\varphi(A) < NA$ le nombre des classes premières; $\varphi(A)$ est donc une généralisation de la fonction φ d'Euler dans la théorie ordinaire des nombres. Entre les propriétés communes des deux fonctions nous indiquons premièrement : *Si* A *et* B *sont des idéaux premiers entre eux, on a* $\varphi(AB) = \varphi(A).\varphi(B)$.

Soient

$$\alpha_1, \ \ldots, \ \alpha_{NA}, \qquad \beta_1, \ \ldots, \ \beta_{NA}$$

des systèmes résiduaires complets pour A et B; d'après le paragraphe 1 on peut déterminer les entiers λ et μ tel que

$$\lambda \equiv 1 \ (\text{mod } A), \qquad \lambda \equiv 0 \ (\text{mod } B); \qquad \mu \equiv 0 \ (\text{mod } A), \qquad \mu \equiv 1 \ (\text{mod } B).$$

Les $NA.NB = N(AB)$ nombres

$$\lambda\alpha_i + \mu\beta_j \qquad (i = 1, 2, \ldots, NA, j = 1, 2, \ldots, NB) \tag{23}$$

forment alors un système résiduaire complet (mod AB), parce qu'on montre facilement qu'ils sont tous différents pour ce module. Cette construction est parfaitement générale et s'applique à la détermination d'un système résiduaire pour un produit quelconque si les facteurs sont premiers entre eux. Si l'on prend dans (23) seulement des α_i

premiers à A et des β_j premiers à B, on obtient $\varphi(A)\varphi(B)$ nombres premiers à A et à B, c'est-à-dire premiers à AB. Une valeur de α_i (ou de β_j) qui n'est première à A (respectivement B) donne toujours un nombre (23) avec un facteur commun avec A (respectivement B).

On peut déterminer $\varphi(A)$ si l'on connaît $\varphi(P^a)$ pour toutes les puissances des idéaux premiers P divisant A. Dans un système résiduaire $(\mathrm{mod}\, P^a)$ tous les nombres sont premiers à P^a, sauf les nombres divisibles par P. Il faut donc déterminer les nombres différents $(\mathrm{mod}\, P^a)$ divisibles par P. Soit π un nombre premier par rapport à P (*voir* § 1), c'est-à-dire un nombre divisible par P, mais non par P^2. Les nombres $\alpha\pi$ ou α prennent les $N(P^{a-1})$ valeurs d'un système de résidus $(\mathrm{mod}\, P^{a-1})$ sont alors tous différents $(\mathrm{mod}\, P^a)$ et tous divisibles par P, et il s'ensuit facilement d'après le paragraphe 1 que tout nombre divisible par P est congru à un nombre de cette forme $(\mathrm{mod}\, P^a)$. On a donc

$$\varphi(P^a) = NP^a - NP^{a-1} = N(P^a)\left(1 - \frac{1}{NP}\right),$$

et pour un idéal général A avec la décomposition

$$A = P_1^{a_1} \dots P_r^{a_r}$$

en facteurs premiers on obtient

$$\varphi(A) = NA\left(1 - \frac{1}{NP_1}\right) \dots \left(1 - \frac{1}{NP_r}\right). \tag{24}$$

Comme pour la fonction φ ordinaire on a

$$\sum_D \varphi(D) = NA,$$

où la somme s'étend sur tous les diviseurs idéaux de A.

Le *théorème de Fermat généralisé* a la forme suivante pour des idéaux : *Chaque nombre γ premier à* A *satisfait la congruence*

$$\gamma^{\varphi(A)} \equiv 1 \ (\mathrm{mod}\, A). \tag{25}$$

Ce théorème est une conséquence directe du fait que les classes résiduaires premières à A forment un groupe abélien d'ordre $\varphi(A)$ par rapport à multiplication. On peut aussi le montrer comme il suit : Soit $\gamma_1, \dots, \gamma_{\varphi(A)}$ un système résiduaire pour les classes premières

à A. Alors tous les produits $\gamma_i\gamma$ sont aussi premiers à A, d'où

$$\gamma_i\gamma \equiv \gamma_j \pmod{A}. \tag{26}$$

On voit aussitôt que deux résidus γ_i et γ_{i_1} correspondent à deux résidus différents (mod A) et la totalité des nombres γ_j est donc la même que la totalité des γ_i. Nous multiplions les congruences (26) pour $i = 1, 2, \ldots, \varphi(A)$ et obtenons

$$\gamma_1 \ldots \gamma_{\varphi(A)}\gamma^{\varphi(A)} \equiv \gamma_1 \ldots \gamma_{\varphi(A)} \pmod{A},$$

et puisque le produit des γ_i est premier à A on en tire la congruence (25).

5. **Systèmes résiduaires pour des idéaux premiers.** — Soit P un idéal premier donné et $NP = p^f$, où f est le degré de P. *Les classes résiduaires* (mod P) *forment un corps abstrait* (1). En effet, soit

$$0, \rho_1, \ldots \rho_{p^f-1} \tag{27}$$

un système résiduaire; les nombres $\rho_i \pm \rho_j$ et $\rho_i\rho_j$ sont congrus a l'un des nombres (27) (mod P) et si $\rho_i \not\equiv 0 \pmod{P}$ on peut toujours trouver un ρ tel que $\rho_i\rho \equiv \rho_j \pmod{P}$. Il est aussi évident que cette propriété est caractéristique pour les idéaux premiers.

Toute la théorie des congruences supérieures pour un nombre premier peut être transférée aux modules premiers P dans un corps algébrique. On considère tous les polynomes

$$f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$$

avec coefficients entiers dans $K(\mathfrak{I})$. On montre sans difficulté que la décomposition de $f(x)$ en facteurs irréductibles (mod P) est unique. Si $f(\rho) \equiv 0 \pmod{P}$, où ρ est un nombre de $K(\mathfrak{I})$, on dit que la congruence $f(x) \equiv 0 \pmod{P}$ a la racine ρ et il existe une décomposition $f(x) \equiv (x - \rho)f_1(x) \pmod{P}$. Une congruence de degré n a au plus n racines (mod P).

D'après (24) et (25) chaque entier γ non divisible par P satisfait la congruence

$$\gamma^{p^f-1} \equiv 1 \pmod{P},$$

(1) Un corps abstrait est un système d'éléments clos par rapport aux quatre opérations fondamentales satisfaisant les axiomes ordinaires pour l'addition, soustraction, multiplication et division.

d'où : tout entier du corps satisfait la congruence

$$x^{p^f} - x \equiv 0 \pmod{\mathrm{P}}. \tag{28}$$

Cette congruence a donc autant de racines différentes que son degré $p^f = \mathrm{NP}$ et l'on a par conséquence

$$x^{p^f} - x \equiv x(x-\rho_1)\dots(x-\rho_{p^f-1}) \pmod{\mathrm{P}}, \tag{29}$$

où les ρ_i sont les nombres du système (27).

A l'autre côté, il est bien connu (1) que

$$x^{p^f} - x \equiv \Pi\varphi(x) \pmod{p}, \tag{30}$$

où le produit s'étend sur tous les polynomes $\varphi(x)$ irréductibles (mod p) à coefficients rationnels, pour lesquels le degré f' est un diviseur de f. Une comparaison des deux identités (29) et (30) nous donne :

Soit $\varphi(x)$ un polynome rationnel irréductible (mod p). *Si le degré f' de $\varphi(x)$ est un diviseur du degré f de l'idéal premier* P, *la congruence* $\varphi(x) \equiv 0$ (mod P) *aura f' racines distinctes.*

Le polynome $\varphi(x)$ se décompose donc en facteurs linéaires (mod P); une généralisation de ce théorème est le suivant : *Un polynome rationnel $\psi(x)$ irréductible* (mod p) *est le produit de d facteurs irréductibles* (mod P) *chacun de degré $\frac{f'}{d}$, où $d = (f', f)$ est le p. g. d. c. du degré f' de $\psi(x)$ et f de* P.

Soit maintenant

$$\varphi(x) = x^f + a_1 x^{f-1} + \dots + a_f \tag{31}$$

un polynome irréductible (mod p) et soit α une racine de la congruence $\varphi(x) \equiv 0$ (mod P). D'après la théorie élémentaire des congruences (mod p), on a

$$\varphi(x)^p \equiv x^{pf} + a_1 x^{p(f-1)} + \dots + a_f = \varphi(x^p) \pmod{p}$$

et parce que P est un diviseur de p on obtient aussi $\varphi(\alpha^p) \equiv 0$ (mod P).

---

(1) Pour les résultats de la théorie des congruences supérieures appliquées dans la suite, il faut renvoyer à I. A. Serret, *Cours d'Algèbre supérieure.*

Toutes les puissances

$$\alpha, \quad \alpha^p, \quad \ldots, \quad \alpha^{p^{f-1}} \tag{32}$$

sont donc des racines de notre congruence; nous allons montrer que les nombres (32) sont tous différents (mod P). D'une congruence

$$\alpha^{p^a} \equiv \alpha^{p^b} \pmod{P}, \qquad b > a,$$

l'on tire en observant que α satisfait la congruence (28)

$$\alpha^{p^{a+f-b}} \equiv \alpha^{p^f} \equiv \alpha \pmod{P},$$

et l'on conclut comme auparavant que α est aussi une racine d'une congruence irréductible $\psi(x) \equiv 0 \pmod{P}$ où le degré de $\psi(x)$ est un diviseur de $f-(b-a)$. Parce que $\psi(x)$ est premier à $\varphi(x) \pmod{p}$, on peut déterminer les polynomes $A(x)$ et $B(x)$ à coefficients rationnels tels que

$$A(x)\varphi(x) + B(x)\psi(x) \equiv 1 \pmod{p},$$

et pour $x = \alpha$ on en tire $0 \equiv 1 \pmod{P}$, ce qui est impossible, P n'étant pas l'idéal unité. Nous avons donc démontré : *Soit α une racine de la congruence irréductible $\varphi(x) \equiv 0 \pmod{P}$ de degré f. Alors on a*

$$\varphi(x) \equiv (x-\alpha)(x-\alpha^p)\ldots(x-\alpha^{p^{f-1}}) \pmod{P}. \tag{33}$$

Les nombres (32) sont appelés parfois les conjugués de $\alpha \pmod{P}$.

C'est à présent possible de donner une représentation très simple d'un système résiduaire $(27) \pmod{P}$. Nous montrerons : *Si α est une racine d'une congruence irréductible* (31) *de degré f, les nombres*

$$C(\alpha) = c_0 + c_1\alpha + \ldots + c_{f-1}\alpha^{f-1} \tag{34}$$
$$(c_i = 0, 1, \ldots, p-1, \; i = 0, 1, \ldots, f-1).$$

forment un système résiduaire (mod P).

Il suffit de montrer que les p^f nombres (34) sont tous différents (mod P); cependant, si $C(\alpha)$ et $C_1(\alpha)$ sont congrus (mod P) on aura $D(\alpha) = C(\alpha) - C_1(\alpha) \equiv 0 \pmod{P}$, sans que les coefficients de $D(x)$ soient tous divisibles par p. $D(x)$ est donc premier au polynome irréductible $\varphi(x) \pmod{P}$ et l'on trouvera comme plus haut

des polynomes $A(x)$ et $B(x)$ tels que

$$A(x)D(x)+B(x)\varphi(x)\equiv 1 \qquad (\mathrm{mod}\, p),$$

d'où résulte pour $x=\alpha$ la congruence impossible $0\equiv 1\ (\mathrm{mod}\ P)$.

Si en général $A(\alpha)$ et $A_1(\alpha)$ sont des polynomes en α, mais de degrés arbitraires, on montrera facilement qu'on a

$$A(\alpha)\equiv A_1(\alpha) \qquad (\mathrm{mod}\, P) \tag{35}$$

seulement si la différence $A(x)-A_1(x)$ est divisible par $\varphi(x)$ $(\mathrm{mod}\ p)$, c'est-à-dire dans la notation de Dedekind

$$A(x)\equiv A_1(x) \qquad [\mathrm{mod}\, p,\ \varphi(x)], \tag{36}$$

et réciproquement (35) est une conséquence de (36). Il y a donc une correspondance univoque entre les classes des résidus (mod P) et les résidus réduits des polynomes à coefficients rationnels pour le module double $[\mathrm{mod}\ p,\ \varphi(x)]$, tel que si $\rho\to R(x)$, $\rho_1\to R_1(x)$ on aura $\rho\pm\rho_1\to R(x)\pm R_1(x)$ et $\rho\rho_1\to R(x)R_1(x)$. *Le corps abstrait formé par les classes résiduaires* (mod P), *où* P *est un idéal premier de degré* f *est isomorphe au corps de* p^f *éléments formés par les résidus réduits des polynomes rationnels* $[\mathrm{mod}\ p,\ \varphi(x)]$, *où* $\varphi(x)$ *est un polynome irréductible de degré* f. Ce dernier type de corps est appelé aussi parfois un corps des *imaginaires de Galois*, défini par Galois par une racine « imaginaire » j d'une congruence « insoluble » dans le corps rationnel $\varphi(x)\equiv 0\ (\mathrm{mod}\ p)$.

On doit à M. Moore le théorème, que chaque corps abstrait d'un nombre fini d'éléments est isomorphe à un corps résiduaire $[\mathrm{mod}\ p, \varphi(x)]$ et puisqu'on peut toujours trouver des corps et des idéaux premiers P d'un degré f quelconque, on en tire : Tout corps abstrait d'un nombre fini d'éléments est isomorphe à un corps de classes résiduaires pour un idéal premier.

Le nombre de représentations (34) des résidus (mod P) est évidemment fN_f où N_f est le nombre de polynomes irréductibles $(\mathrm{mod}\, p)$ de degré f; de la théorie des congruences supérieures on sait que

$$N_f=\frac{1}{f}\left(p^f-\sum_i p^{\frac{f}{p_i}}+\sum_{i\neq j} p^{\frac{f}{p_i p_j}}-\dots\right), \tag{37}$$

où $p_1, p_2, \dots$ sont les nombres premiers différents divisant f.

Il y a aussi d'autres représentations utiles d'un système résiduaire (mod P). Nous avons vu que chaque entier $\alpha\not\equiv 0\ (\mathrm{mod}\ P)$ satisfait à

la congruence

$$\alpha^{p^f-1} \equiv 1 \pmod{P}. \tag{38}$$

Par les mêmes procédés qu'on applique dans la théorie ordinaire des nombres, on montre l'existence d'une solution *primitive* α de la congruence (38), c'est-à-dire une solution α qui ne satisfait aucune congruence

$$\alpha^l \equiv 1 \pmod{P},$$

où $l < p^f - 1$. Il s'ensuit que les puissances

$$1, \ \alpha, \ \alpha^2, \ \ldots, \ \alpha^{p^f-2} \tag{39}$$

sont toutes différentes (mod P) et les $p^f - 1$ nombres (39) forment un système résiduaire (mod P) pour tous les nombres non divisibles par P. On peut aussi l'exprimer ainsi : *Le groupe multiplicatif des classes des résidus* (mod P) *non divisible par* P *est cyclique d'ordre* $p^f - 1$. Il y a $\varphi(p^f - 1)$ nombres primitifs (mod P), où φ est la fonction d'Euler.

On peut aussi demander s'il existe des nombres α tels que les conjugués (32) de α (mod P) forment une base du système résiduaire, c'est-à-dire, chaque nombre est congru (mod P) à l'un des nombres

$$c_0\alpha + c_1\alpha^p + \ldots + c_{f-1}\alpha^{p^{f-1}} \qquad (c_i = 0, 1, \ldots, p-1).$$

Eisenstein (1850) a déjà proposé un problème équivalent et Schönemann en donna une solution dans un cas spécial. Dans le cas général, Hensel [2] a montré l'existence de tels nombres; on en trouvera une démonstration plus simple chez Ore [3].

6. **Systèmes résiduaires** (mod P^a). — Si l'on connaît un système résiduaire (mod P) et un nombre premier π par rapport à P, on peut facilement déterminer un système résiduaire pour toutes les puissances de P. Supposons que le système résiduaire (mod P) est donné sous la forme (34); on a donc pour un entier arbitraire

$$\omega \equiv C_0(\alpha) \pmod{P},$$

ou bien $\omega = C_0(\alpha) + \lambda_1$, où $\lambda_1 \equiv 0 \pmod{P}$. Il existe par suite une solution γ_1 de la congruence $\lambda_1 \equiv \pi\gamma_1 \pmod{P^2}$ et si $\gamma_1 \equiv C_1(\alpha) \pmod{P}$, on en tire

$$\omega \equiv C_0(\alpha) + C_1(\alpha)\pi \pmod{P^2}.$$

De cette congruence on conclut

$$\omega - C_0(\alpha) - C_1(\alpha)\pi = \lambda_2,$$

où $\lambda_2 \equiv 0 \pmod{P^2}$ et γ_2 se détermine par $\lambda_2 \equiv \gamma_2 \pi^2 \pmod{P^3}$ etc.

Chaque nombre ω peut être représenté dans la forme

$$\omega \equiv C_0(\alpha) + C_1(\alpha)\pi + \ldots + C_{a-1}(\alpha)\pi^{a-1} \pmod{P^a}. \tag{39}$$

Il y a $p^{af} = NP^a$ nombres différents $(39) \pmod{P^a}$ et ils constituent donc un système résiduaire $(\text{mod } P^a)$.

Le nombre α est une racine de la congruence $\varphi(x) \equiv 0 \pmod{P}$; nous allons montrer qu'on peut toujours choisir α tel que $\pi = \varphi(\alpha)$. En effet, si $\varphi(\alpha) \equiv 0 \pmod{P^2}$, on posera $\alpha' = \alpha + \pi$; parce que $\alpha' \equiv \alpha \pmod{P}$ les nombres (34) avec α' remplaçant α forment encore un système résiduaire $(\text{mod } P)$, et

$$\varphi(\alpha') = \varphi(\alpha) + \pi\varphi'(\alpha) + \frac{\varphi''(\alpha)}{2!}\pi^2 + \ldots + \pi^f. \tag{40}$$

On sait que les coefficients de $\frac{\varphi^{(i)}(x)}{i!}$ sont tous entiers et l'on obtient donc de (40) d'après notre supposition sur $\varphi(\alpha)$

$$\varphi(\alpha') \equiv \pi\varphi'(\alpha) \pmod{P^2};$$

ici le nombre $\varphi'(\alpha)$ n'est pas divisible par P, ce qu'on déduit comme plus haut du fait que $\varphi(x)$ et $\varphi'(x)$ sont premiers entre eux $(\text{mod } p)$; $\varphi(\alpha')$ est par conséquence un nombre premier par rapport à P.

On obtient une représentation canonique importante de l'idéal premier P en faisant un choix encore plus spécial du nombre α. Le nombre premier p divisible par P est en général aussi divisible par des idéaux premiers différents $P_2, P_3, \ldots$. Nous avons choisi α tel que $\varphi(\alpha)$ est divisible par P, maisn on par P^2; d'après le paragraphe 1, il est toujours possible de determiner un entier α'' tel que

$$\alpha'' \equiv \alpha \pmod{P^2}, \qquad \alpha'' \equiv 0 \pmod{P_i} \qquad (i = 2, 3, \ldots).$$

Le nombre $\varphi(\alpha'')$ est aussi divisible par P, mais non par P^2; pour les idéaux P_i on aura $\varphi(\alpha'') \equiv \varphi(0) \pmod{P_i}$ et le nombre rationnel $\varphi(0)$ n'est pas divisible par p, parce qu'on en déduit que la fonction irréductible $\varphi(x)$ sera divisible par $x \pmod{p}$. Dans le cas exceptionnel $\varphi(x) = x$ on peut mettre

$$\alpha'' \equiv \alpha \pmod{P}, \qquad \alpha'' \equiv 1 \pmod{P_i} \qquad (i = 2, 3, \ldots).$$

Le résultat de ces considérations est donc : *Soit* P *un idéal premier*, $NP = p^f$ *et soit* $\varphi(x)$ *un polynome irréductible* $(\mathrm{mod}\, p)$ *de degré* f. *Alors on peut déterminer un entier* α *tel que*

$$P = [p, \varphi(\alpha)]. \tag{41}$$

Revenons cependant au système résiduaire (39) $(\mathrm{mod}\, P^a)$, et supposons que l'ordre de l'idéal premier P est e, c'est-à-dire p est divisible exactement par P^e. Si l'on considère des congruences $(\mathrm{mod}\, P^a)$ où $a \geqq e$ il est souvent commode d'appliquer une forme quelque peu différente du système résiduaire (39). On a évidemment pour un entier arbitraire

$$\omega = C_0^{(0)}(\alpha) + C_1^{(0)}(\alpha)\pi + \ldots + C_{e-1}^{(0)}(\alpha)\pi^{e-1} + \lambda_1,$$

où $\lambda_1 \equiv 0 (\mathrm{mod}\, P^e)$. Il existe par conséquent une solution γ_1 de la congruence $\lambda_1 \equiv p\gamma_1 (\mathrm{mod}\, P^a)$ et dans la même manière on aura

$$\gamma_1 = C_0^{(1)}(\alpha) + C_1^{(1)}(\alpha)\pi + \ldots + C_{e-1}^{(1)}(\alpha)\pi^{e-1} + \lambda_2,$$

où $\lambda_2 \equiv 0 (\mathrm{mod}\, P^e)$ et $\lambda_2 \equiv p\gamma_2 (\mathrm{mod}\, P^a)$, etc. En continuant, on obtient

$$\omega \equiv D_0(\alpha) + D_1(\alpha)\pi + \ldots + D_{e-1}(\alpha)\pi^{e-1} \quad (\mathrm{mod}\, P^a), \tag{42}$$

où $D_i(\alpha)$ sont des polynomes en α à coefficients rationnels entiers et de degré $< f$.

Supposons à présent $\pi = \varphi(\alpha)$; de (42) il s'ensuit

$$\omega \equiv D(\alpha) \quad (\mathrm{mod}\, P^a), \tag{43}$$

où $D(x)$ est un polynome à coefficients entiers et rationnels. Tous les nombres de la forme $D(\alpha)$ forment évidemment un *anneau* (*voir* § 1, Chap. II) que je dénoterai par $A(\alpha)$. Tout entier du corps est donc congru à un nombre de $A(\alpha)$ $(\mathrm{mod}\, P^a)$, où l'exposant a est arbitraire; j'appellerai $A(\alpha)$ un anneau *représentatif* par rapport à P.

Il est facile de trouver la condition nécessaire et suffisante pour qu'un anneau $A(\alpha)$ soit représentatif par rapport à P. Soit en effet $\varphi(\alpha)$ un nombre de $A(\alpha)$ de degré minimal tel que $\varphi(\alpha)$ est divisible par P. Le polynome $\varphi(x) \not\equiv 0 (\mathrm{mod}\, p)$ sera alors irréductible $(\mathrm{mod}\, p)$, parce qu'une congruence $\varphi(x) \equiv \psi_1(x)\psi_2(x) (\mathrm{mod}\, p)$ montrera que $\psi_1(\alpha)$ ou $\psi_2(\alpha)$ est divisible par P. Soit maintenant $D(\alpha)$ un nombre

arbitraire de $A(\alpha)$; nous divisons $D(\alpha)$ par $\varphi(\alpha)$

$$D(\alpha) \equiv Q(\alpha)\varphi(\alpha) + r(\alpha) \pmod{p},$$

d'où $D(\alpha) \equiv r(\alpha) \pmod{P}$ où $r(\alpha)$ est l'un des nombres

$$r(\alpha) = c_0 + c_1\alpha + \ldots + c_{f_1-1}\alpha^{f_1-1}, \qquad (c_i = 0, 1, \ldots, p-1),$$

f_1 indiquant le degré de $\varphi(x)$. On peut montrer comme plus haut que les p^{f_1} nombres $r(\alpha)$ sont différents (mod P) et parce que $A(\alpha)$ doit contenir tous les résidus (mod P) on en conclut $f_1 = f$. Il faut encore assurer, que $A(\alpha)$ contient un nombre premier π par rapport à P. Si l'ordre de P est $e = 1$, le nombre premier p est déjà divisible exactement par P. Si $e > 1$ il faut que $\pi = \varphi(\alpha)$. Soit en effet $D(\alpha)$ un nombre divisible par P; on trouve que

$$D(\alpha) \equiv Q(\alpha)\varphi(\alpha) \pmod{p}$$

et si $\varphi(\alpha) \equiv 0 \pmod{P^2}$ tous les nombres de $A(\alpha)$ divisibles par P seront aussi divisibles par P^2 et $A(\alpha)$ ne contient aucun nombre π. *L'anneau* $A(\alpha)$ *est un anneau représentatif par rapport à* P *seulement si* α *est une racine d'une congruence irréductible* $\varphi(x) \equiv 0 \pmod{P}$ *de degré* f *et* $\varphi(\alpha) \not\equiv 0 \pmod{P^2}$ *si l'ordre de* P *est* $e > 1$.

Le traitement des congruences $(\mathrm{mod}\ P^a)$ se simplifie considérablement lorsqu'on connaît un anneau représentatif $A(\alpha)$. Observons d'abord, qu'il n'est pas nécessaire de considérer en $A(\alpha)$ des nombres $D(\alpha)$ de degré en α excédant $ef - 1$; il s'ensuit en effet de (42) pour $\pi = \varphi(\alpha)$, qu'un nombre arbitraire ω est congru à un nombre $D(\alpha)$ de degré plus petit que ef; dans la suite nous supposons que les nombres $D(\alpha)$ considérés soient tous de cette forme.

Soit $\omega \equiv D(\alpha) \pmod{P^a}$ et cherchons la condition pour que ω soit divisible par P^b, $b \leq a$. Soit premièrement $b < e$; alors $D(x) \not\equiv 0 \pmod{p}$ parce que si tous les coefficients de $D(x)$ sont divisibles par p, ω contiendra au moins la puissance P^e de P. Si $D(x) \equiv \varphi(x)^\beta\, Q(x) \pmod{p}$ où $Q(x)$ n'est pas divisible par $\varphi(x) \pmod{p}$, il faut évidemment que $\beta = b$ et cette condition est aussi suffisante.

Supposons ensuite $b \geq e$; il est clair que $D(x)$ sera divisible par une puissance de p et l'on vérifie facilement le résultat : un nombre

$D(\alpha)$ est divisible exactement par P^b seulement si $D(x)$ a la forme

$$D(x) \equiv p^q \varphi(x)^r Q(x) \qquad (\mathrm{mod}\, p^{q+1}),$$

où $Q(x)$ n'est pas divisible par $\varphi(x)$ (mod p) et $b = eq + r$, $0 \leqq r < e$. Ces remarques s'appliquent aussi aux congruences

$$B(\alpha) \equiv C(\alpha) \qquad (\mathrm{mod}\, P^b),$$

et l'on peut décider quand une congruence de cette forme aura lieu. Si l'on connaît un anneau représentatif par rapport à P, l'étude des congruences pour des puissances de P est donc réduite à l'étude des congruences supérieures ordinaires (mod p). Dans le problème de la détermination de la décomposition d'un nombre premier p en facteurs idéaux premiers, on ne demande donc seulement de connaître les ordres et les degrés des idéaux premiers, mais aussi la connaissance d'un nombre α tel que $A(\alpha)$ soit représentatif, ou plus spécial encore, un nombre α pour chaque idéal premier P tel que $P = [p, \varphi(\alpha)]$. On peut aussi caractériser les anneaux représentatifs dans une manière plus algébrique. D'après le critère déduit pour un tel anneau on sait que le nombre $\varphi(\alpha)^e$ est divisible exactement par P^e, si $e > 1$, et dans le cas $e = 1$ il peut même contenir une puissance supérieure de P. Il existe donc en tout cas une solution γ de la congruence

$$\varphi(\alpha)^e \equiv -p\gamma \qquad (\mathrm{mod}\, P^a),$$

où $\gamma \not\equiv 0$ (mod P) si $e > 1$; pour γ on aura comme plus haut

$$\gamma \equiv M(\alpha) \qquad (\mathrm{mod}\, P^a)$$

et il résulte : *Si le nombre α définit un anneau représentatif par rapport à* P, *il satisfait une congruence rationnelle de degré ef*

$$F(x) = \varphi(x)^e + pM(x) \equiv 0 \qquad (\mathrm{mod}\, P^a), \tag{44}$$

où $\varphi(x)$ est une fonction irréductible (mod p) *de degré f, et le degré de $M(x)$ est $< ef$ et $M(x) \not\equiv 0$ [mod p, $\varphi(x)$] si $e > 1$.*

Le polynome $M(x)$ dépend naturellement de l'exposant a. Réciproquement il s'ensuit facilement, qu'une racine d'une congruence (44), $a > e$, donnera toujours un anneau représentatif.

Pour $e = 1$ le polynome $F(x)$ est évidemment irréductible (mod p).

Il est d'intérêt de noter que si $e > 1$, $F(x)$ sera irréductible (mod p^2) et par conséquence pour chaque puissance supérieure de p (théorème de Schœnemann). La démonstration en est simple; supposons $F(x) \equiv G(x)H(x) \pmod{p^2}$. La factorisation (mod p) est unique, et les facteurs $G(x)$ et $H(x)$ sont donc de la forme

$$G(x) = \varphi(x)^b + pL(x), \qquad H(x) = \varphi(x)^c + pN(x), \qquad b + c = e.$$

Nous formons leur produit et la comparaison avec (44) nous donne

$$L(x)\varphi(x)^c + N(x)\varphi(x)^b \equiv M(x) \qquad (\mathrm{mod}\, p),$$

d'où $M(x) \equiv 0\ [\mathrm{mod}\ p, \varphi(x)]$ contre la supposition.

Observons enfin que chaque nombre du corps doit satisfaire à une congruence rationnelle de degré ef (mod P^a); en effet, soit γ un entier arbitraire et

$$\gamma \equiv a_{0,0} + a_{0,1}\alpha + \ldots + a_{0,ef-1}\alpha^{ef-1} \qquad (\mathrm{mod}\, P^a)$$

la représentation dans l'anneau représentatif. On obtient dans la même manière

$$\begin{aligned} \gamma\alpha &\equiv a_{1,0} + a_{1,1}\alpha + \ldots + a_{1,ef-1}\alpha^{ef-1} \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \gamma\alpha^{ef-1} &\equiv a_{ef-1,0} + a_{ef-1,1}\alpha + \ldots + a_{ef-1,ef-1}\alpha^{ef-1} \end{aligned} \qquad (\mathrm{mod}\, P^a),$$

d'où comme dans le paragraphe 3 (Chap. II),

$$\begin{vmatrix} a_{0,0} - \gamma & a_{0,1} & \ldots & a_{0,ef-1} \\ a_{1,0} & a_{1,1} - \gamma & \ldots & a_{1,ef-1} \\ a_{ef-1,0} & \ldots\ldots & \ldots & a_{ef-1,ef-1} - \gamma \end{vmatrix} \equiv 0 \qquad (\mathrm{mod}\, P^a),$$

ce qui est la congruence cherchée.

7. **Racines primitives.** — Nous avons jusqu'à présent considéré les systèmes résiduaires complets et le groupe additif correspondant; revenons d'abord aux classes premières au module A étudiées dans le paragraphe 4. Nous avons déjà vu qu'ils forment un groupe abélien G_A d'ordre $\varphi(A)$ par rapport à multiplication; c'est alors un problème important de trouver sous quelle condition G_A sera cyclique, c'est-à-dire quand il existe une *racine primitive* $\rho\ (\mathrm{mod}\, A)$ telle que les puissances $\rho^i [i = 0, 1, \ldots, \varphi(A) - 1]$ représentent toutes les classes premières (mod A). Ce problème est évidemment un cas

spécial du problème plus général de la détermination des invariants du groupe G_A.

On voit facilement, comme pour le problème correspondant dans la théorie ordinaire des nombres, que si

$$A = P_1^{a_1} \dots P_r^{a_r} \tag{45}$$

est la décomposition de A en facteurs premiers, le groupe G_A sera le produit direct des groupes G_{P^a}

$$G_A = G_{P^{a_1}} \times \dots \times G_{P^{a_r}}. \tag{46}$$

Tous les nombres premiers à A satisfont la congruence

$$\rho^{\varphi(A)} \equiv 1 \pmod{A},$$

et les racines primitives sont caractérisées par la propriété qu'ils ne satisfont à aucune congruence $\rho^l \equiv 1 \pmod{A}$ où $0 < l < \varphi(A)$.

Il suffit, d'après (46), d'étudier les groupes G_{P^a} d'ordre

$$\varphi(P^a) = NP^{a-1}(NP - 1) = p^{f(a-1)}(p^f - 1).$$

S'il existe une racine primitive $\rho \pmod{P^a}$, ce nombre sera aussi une racine primitive pour chaque puissance inférieure de P. Du paragraphe 5 on tire : 1° *Il existe toujours des racines primitives* (mod P).

Dans la théorie ordinaire des nombres il y a des racines primitives pour chaque puissance d'un nombre premier; il n'en est pas ainsi pour les puissances de tous les idéaux premiers.

Soit ρ une racine primitive (mod P), par conséquent

$$\rho^{p^f-1} \equiv 1 \pmod{P}, \qquad \rho^{p^f} = 1 + \lambda, \qquad \lambda \equiv 0 \pmod{P}.$$

Nous allons examiner quand ρ peut être une racine primitive $(\text{mod } P^2)$, c'est-à-dire quand $\rho^l \equiv 1 \pmod{P^2}$ seulement pour $l \geq p^f(p^f - 1)$. Il faut évidemment que $\lambda \not\equiv 0 \pmod{P^2}$, et l'on peut toujours trouver un ρ tel que cette condition soit satisfaite; il suffit, si $\lambda \equiv 0 \pmod{P^2}$, de remplacer ρ par $\rho + \pi$ où π est un nombre premier par rapport à P. On aura alors

$$\rho^{k(p^f-1)} = (1+\lambda)^k = 1 + \binom{k}{1}\lambda + \binom{k}{2}\lambda^2 + \dots + \lambda^k, \tag{47}$$

et par conséquent

$$\rho^{p(p^f-1)} \equiv 1 \pmod{P^2}.$$

On en conclut : 2° *Il existe des racines primitives* (mod P^2) *seulement si* $f = 1$, *c'est-à-dire* $NP = p$.

Si P est un idéal du premier degré divisant $p \neq 2$, et si l'ordre de P est $e > 1$, il n'existe pas des racines primitives pour des puissances supérieures de P. De (47) on obtient en effet pour $f = 1$ et $k = p$

$$\rho^{p(p-1)} \equiv 1 \qquad (\mathrm{mod}\, P^3).$$

Nous montrerons enfin par induction : 3° *Si* $NP = p \neq 2$ *et* $e = 1$ *il existe des racines primitives pour chaque puissance de* P. Soit ρ une racine primitive (mod P^a)

$$\rho^{p^{a-1}(p-1)} \equiv 1 \qquad (\mathrm{mod}\, P^a), \qquad \rho^{p^{a-1}(p-1)} = 1 + \lambda_a,$$

et supposons $\lambda_a \not\equiv 0 \,(\mathrm{mod}\, P^{a+1})$. Par une expansion analogue à (47), on obtient

$$\rho^{kp^{a-1}(p-1)} \equiv 1 + k\lambda_a \qquad (\mathrm{mod}\, P^{a+1}),$$

ce qui donne $k = p$ pour l'exposant minimal; pour $k = p$ on tire aussi facilement

$$\rho^{p^a(p-1)} \equiv 1 + p\lambda_a \equiv 1, \qquad \lambda_{a+1} \not\equiv 0 \qquad (\mathrm{mod}\, P^{a+2}),$$

ce qui complète l'induction.

Dans le cas $p = 2$ on trouve : 4° *Il y a des racines primitives* (mod P^1), $NP = 2$, *seulement si l'ordre de* P *est* $e > 1$. Pour un module P^a, $a > 3$, $p = 2$ il n'y a pas de racines primitives.

Les cas 1° à 4° complètent la détermination des racines primitives pour les puissances d'un idéal premier, et l'on en déduit sans difficultés tous les idéaux (45) ayant telles racines. Il faut et il suffit, d'après un théorème sur les groupes abéliens, que les ordres des groupes G_{P^a} en (46) soient tous premiers entre eux, et qu'il existe des racines primitives pour chaque P^a. Il s'ensuit de ce critère que A ne peut pas contenir qu'un seul idéal P ne divisant pas 2, parce que $\varphi(P^a) = p^{f(a-1)}(p^f - 1)$, $p > 2$ est toujours pair. $\varphi(P^a)$ est impair seulement pour $a = 1$, $p = 2$, d'où l'on tire les cas possibles. Les résultats précédents sont dus à Wiman, mais les mêmes résultats ont été retrouvés par un grand nombre d'auteurs (Westlund, Ranum, Metrod, Strauch, etc.).

G. Wolf étudia le premier les invariants d'un groupe G_{P^a} et ses résultats furent complétés par Takenouchi. Si ρ est une racine pri-

mitive (mod P) on aura, pour chaque nombre γ premier à P,

$$\gamma \equiv \rho^l \lambda \qquad (\mathrm{mod}\, \mathrm{P}^a),$$

où $\lambda \equiv 1 \ (\mathrm{mod}\, \mathrm{P})$. Les λ forment aussi un groupe multiplicatif et G_{p^n} sera donc le produit direct d'un groupe cyclique d'ordre $p^f - 1$ et un groupe abélien G^l d'ordre $p^{(a-1)f}$. Les invariants de G^l sont des puissances de p et pour $a > e + \left[\frac{e}{p-1}\right]$ leur nombre est $ef+1$ ou ef selon qu'il existe une solution ou non de la congruence

$$x^{p-1} + p \equiv 0 \qquad (\mathrm{mod}\, \mathrm{P}^{e+1})$$

dans le corps. Pour des valeurs plus petites de a, le nombre des invariants dépend de a.

Il faut mentionner ici les belles recherches de Hensel [3]-[7] sur la détermination d'une base multiplicative de G_{p^n} et la représentation correspondante des nombres $(\mathrm{mod}\, \mathrm{P}^a)$ comme un produit des puissances de certains nombres fondamentaux. De cette représentation s'ensuivent simplement les résultats indiqués sur les invariants.

CHAPITRE V.

LES UNITÉS.

Dans le paragraphe 1 (Chap. III) nous avons déjà déduit quelques-unes des propriétés des unités d'un corps $K(\Im)$; dans la suite, je donnerai la démonstration du *théorème fondamental de Dirichlet* sur les unités.

Une unité ε est définie par $N(\varepsilon) = \pm 1$; le produit et le quotient de deux unités sont donc aussi des unités. Soient

$$\varepsilon_1, \quad \varepsilon_2, \quad \ldots, \quad \varepsilon_t \tag{1}$$

des unités du corps; alors tous les nombres

$$\varepsilon = \rho \varepsilon_1^{a_1} \ldots \varepsilon_t^{a_t}$$

sont aussi des unités, les exposants a_l étant entiers rationnels et ρ une

racine d'unité quelconque du corps. Les t unités (1) sont dites indépendantes s'il n'existe aucune relation

$$\varepsilon_1^{b_1} \dots \varepsilon_t^{b_t} = 1 \tag{2}$$

avec des exposants entiers. Dans ce cas, il n'existe même pas de relations

$$\varepsilon_1^{c_1} \dots \varepsilon_t^{c_t} = \rho \tag{3}$$

avec des exposants c_i rationnels, parce qu'une puissance de (3) donnera (2).

Soient maintenant $\mathrm{K}^{(i)}$ $(i = 1, 2, \dots, n)$ les n corps conjugués du corps donné et supposons que l'énumération soit choisie telle que $\mathrm{K}^{(1)}, \dots, \mathrm{K}^{(r_1)}$ soient les corps réels et $\mathrm{K}^{(r_1+1)}, \dots, \mathrm{K}^{(n)}$ les corps complexes. Il y a donc r_1 corps réels et $2r_2 = n - r_1$ corps complexes correspondant aux n racines de l'équation caractéristique du corps K. Supposons enfin que l'énumération des corps complexes est telle que si

$$\mathrm{K}^{(r_1+t)} = \mathrm{K}(\vartheta^{(r_1+t)}) = \mathrm{K}(\alpha + i\beta) \qquad (t = 1, 2, \dots, r_2),$$

alors

$$\mathrm{K}^{(r_1+r_2+t)} = \mathrm{K}(\vartheta^{(r_1+r_2+t)}) = \mathrm{K}(\alpha - i\beta)$$

et posons

$$r = r_1 + r_2 - 1. \tag{4}$$

Le théorème de Dirichlet s'énonce ainsi :

Il existe dans K r *unités fondamentales indépendantes* $\varepsilon_1, \dots, \varepsilon_r$ *tel que toutes les unités peuvent être représentées dans une manière unique sous la forme*

$$\eta = \rho\varepsilon_1^{a_1} \dots \varepsilon_r^{a_r},$$

où les exposants a_i *sont rationnels et entiers et* ρ *est l'une des racines d'unité du corps.*

La démonstration se compose de deux parties. J'éviterai dans la suite la méthode ordinaire introduisant les logarithmes des valeurs absolues des unités; la première partie de la démonstration est fondée sur la généralisation suivante du théorème de Kronecker sur les racines d'unité dans un corps :

Il existe pour chaque corps $K(\Im)$ *un nombre réel positif* δ_k *tel que si les valeurs absolues* $|\omega^{(i)}|\,(i=1, 2, \ldots, n)$ *des conjugués d'un entier* ω *sont toutes plus petites que* $1+\delta_k$, ω *sera nécessairement une racine d'unité.*

En effet, il n'y a qu'un nombre fini R_M d'entiers du corps tel que $|\omega^{(i)}| < M (i=1, 2, \ldots, n)$. Soit $M=2$ et choisissons δ_k aussi petit que

$$(1+\delta_k)^{R_2+1} < 2;$$

soit d'avantage ω un entier tel que $|\omega^{(i)}| < 1+\delta_k$. Les valeurs absolues des conjugués de $\omega^a (a=1, 2, \ldots, R_2+1)$ sont donc toutes plus petites que $(1+\delta_k)^a < 2$ et il y a donc deux exposants a et b tels que $\omega^a = \omega^b$ (C. Q. F. D). On voit aussi qu'on peuttoujours trouver une borne inférieure pour δ_k dépendant seulement du degré n de K. La détermination actuelle de δ_k pour un corps donné sera un problème très intéressant.

Soit maintenant η une unité dépendante des t unités (1), c'est-à-dire

$$\eta^N \varepsilon_1^{a_1} \ldots \varepsilon_t^{a_t} = 1, \tag{5}$$

ou bien pour η et ses conjugués

$$\eta^{(i)} = \rho_t \varepsilon_1^{(i) r_1} \ldots \varepsilon_t^{(i) r_t} \qquad (i=1, 2, \ldots, n) \tag{6}$$

où ρ_t sont des racines d'unité et $r_1, \ldots, r_t$ des exposants rationnels. Nous allons montrer qu'on peut toujours supposer que l'exposant N en (5) n'excède pas une borne fixe dépendante seulement des unités (1). De (6) on tire

$$|\eta^{(i)}| = |\varepsilon_1^{(i)}|^{r_1} \ldots |\varepsilon_t^{(i)}|^{r_t} \qquad (i=1, 2, \ldots, n). \tag{7}$$

Nous étudierons un peu plus généralement une unité η du corps satisfaisant avec ses conjugués des relations (7) avec des exposants réels quelconques.

Soient $y, x_1 \ldots x_t$ des entiers arbitraires; alors

$$\eta' = \eta^y \varepsilon_1^{-x_1} \ldots \varepsilon_t^{-x_t}$$

sera aussi une unité du corps et l'on aura, d'après (7),

$$|\eta'^{(i)}| = |\varepsilon_1^{(i)}|^{y r_1 - x_1} \ldots |\varepsilon_t^{(i)}|^{y r_t - x_t}. \tag{8}$$

Les $t+1$ formes linéaires

$$L_1 = yr_1 - x_1, \quad \ldots, \quad L_t = yr_t - x_t, \quad L_{t+1} = y$$

ont le déterminant ± 1 et d'après le théorème de Minkowski (§ 6, Chap. II) on peut choisir des valeurs entières $y, x_1 \ldots x_t$ tel que pour un $\delta > 0$ arbitraire

$$|L_i| < \delta, \quad (i = 1, 2, \ldots, t), \qquad |y| \leqq \delta^{-t}.$$

En prenant δ suffisamment petit on peut faire les valeurs conjuguées de η' en (8) plus petites que $1+\delta_k$, et par conséquent $\eta' = \sigma$ où σ est une racine d'unité du corps.

Toute unité dépendante des t unités (1) est donc représentable dans la forme

$$\eta = \sigma^{\frac{x_0}{M}} \varepsilon_1^{\frac{x_1}{M}} \ldots \varepsilon_t^{\frac{x_t}{M}} \tag{9}$$

avec un M fixe; cette représentation est unique si les ε_i sont indépendants. Cette représentation (9) nous permet aussi de trouver une base pour toutes les unités dépendantes de (1). Les nombres (9) n'appartiennent pas tous pour des x entiers arbitraires au corps donné, mais on peut, en examinant tous η avec $|x_i| < M$, trouver toutes les unités du corps expressibles dans cette manière. Par un procédé analogue à la détermination d'une base minimale (§ 5, Chap. II), on détermine des unités $\zeta_1, \ldots, \zeta_t$ tel que

$$\zeta_i = \sigma_i^{\frac{x_0^{(i)}}{M}} \varepsilon_1^{\frac{x_1^{(i)}}{M}} \ldots \varepsilon_t^{\frac{x_t^{(i)}}{M}} \qquad (i = 1, 2, \ldots, t),$$

et tel que $x_i^{(i)}$ soit l'exposant minimal pour une unité du corps expressible dans cette forme. Il s'ensuit alors sans difficulté : *Soit* (1) *un système de t unités indépendantes du corps; il est possible de trouver t unités indépendantes* $\zeta_1 \ldots \zeta_t$ *de sorte que chaque unité dépendante de* (1) *est représentable uniquement dans la forme*

$$\eta = \sigma \xi_1^{a_1} \ldots \xi_t^{a_t},$$

où σ *est une racine d'unité du corps et les* a_i *des exposants entiers.* J'observe aussi sans en discuter les détails qu'on peut, au moins théoriquement, calculer une base d'un système (1) donné par un nombre fini d'opérations.

La seconde partie de la démonstration du théorème de Dirichlet

est de montrer que le nombre maximal d'unités indépendantes est r. Il est assez facile de montrer que ce nombre ne peut pas excéder r. En effet, $r+1$ unités $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_r$ sont dépendantes s'il existe r relations

$$|\varepsilon_0^{(i)}|^{c_0} \ldots |\varepsilon_r^{(i)}|^{c_r} = 1 \qquad (i = 1, 2, \ldots, r), \tag{10}$$

avec des exposants c_i réels quelconques, parce que de $N(\varepsilon_i) = \pm 1$ on conclut que (10) est vrai même pour $i = r+1$, d'où

$$|\varepsilon_0^{(i)}| = |\varepsilon_1^{(i)}|^{a_1} \ldots |\varepsilon_r^{(i)}|^{a_r} \qquad (i = 1, 2, \ldots, n).$$

Mais il est toujours possible de trouver $r+1$ nombres réels $c_0, c_1, \ldots, c_r$ tels que (10) soit satisfait avec des exposants qui ne sont pas tous nuls (1).

La démonstration s'achève en montrant l'existence de r unités indépendantes. Soit d'abord d le discriminant du corps et $\varkappa_1, \ldots, \varkappa_n$ n nombres réels, positifs tels que

$$\varkappa_1 \ldots \varkappa_n = |\sqrt{d}|, \qquad \varkappa_{r_1+l} = \varkappa_{r_1+r_2+l} \qquad (l = 1, 2, \ldots, r_2). \tag{11}$$

Du théorème de Minkowski pour des formes complexes (§ 6, Chap. II), on conclut l'existence d'un entier λ du corps tel que ses conjugués satisfont au

$$|\lambda^{(i)}| \leqq \varkappa_i \quad (i = 1, 2, \ldots, n) \qquad |N(\lambda)| \leqq |\sqrt{d}|.$$

D'après (9) il est évident que $r_1 + r_2 - 1 = r$ des nombres $\varkappa$ sont arbitraires et le reste sera déterminé par (11). Il y a donc un nombre infini d'entiers λ de sorte que $|N(\lambda)| \leqq \sqrt{d}$, si $r > 0$. On sait d'abord qu'il n'y a qu'un nombre fini d'idéaux à norme fixe (§ 2, Chap. IV) et il faut donc que les λ soient associés à un nombre fini $\lambda_1, \lambda_2, \ldots, \lambda_h$ entre eux, c'est-à-dire

$$\lambda = \varepsilon \lambda_k \tag{12}$$

où ε est une unité. Soit alors

$$l \leqq |\lambda_k^{(i)}| \qquad (i = 1, 2, \ldots, n, \; k = 1, 2, \ldots, h),$$

(1) Ce résultat s'ensuit en prenant le logarithme de (10) et l'on en tire un système homogène avec $r+1$ inconnus, les coefficients du système étant les logarithmes des valeurs absolues des unités ε_i. Si l'on veut éviter l'introduction des logarithmes on peut obtenir le même résultat en exécutant l'élimination correspondante sous la forme multiplicative (10).

le minimum des conjugués de λ, et soit a un entier fixe $1 \leqq a \leqq r_1 + r_2$. D'après le théorème de Minkowski, on peut trouver un entier λ tel que

$$|\lambda^{(i)}| < l \quad (i = 1, 2, \ldots, r_1 + r_2) \qquad |N(\lambda)| \leqq |\sqrt{d}|,$$

sauf pour $i = a$. De (12) on en tire pour l'unité correspondante

$$|\varepsilon_a^{(i)}| = |\lambda^{(i)}|\,|\lambda_k^{(i)}|^{-1} < 1 \qquad (i \neq a),$$

et pour $i = a$ on aura $|\varepsilon_a^{(a)}| > 1$ à cause de la condition $N(\varepsilon) = \pm 1$. Nous avons donc montré : *Il existe* $r + 1$ *unités* $\varepsilon_1, \ldots, \varepsilon_{n+1}$ *telles que*

$$|\varepsilon_j^{(i)}| < 1, \qquad (i \neq j) \qquad |\varepsilon_i^{(i)}| > 1. \tag{13}$$

Nous ferons voir que les r unités $\varepsilon_1, \ldots, \varepsilon_r$ sont indépendantes (Minkowski) [4]. Soit en effet

$$\varepsilon_1^{x_1} \ldots \varepsilon_r^{x_r} = 1,$$

ou bien en séparant les exposants positifs et les exposants négatifs

$$\prod_{\alpha} \varepsilon_\alpha^{\gamma_\alpha} = \prod_{\beta} \varepsilon_\beta^{\gamma_\beta} \tag{14}$$

où tous les γ sont positifs et chaque nombre $1, 2, \ldots, r$ appartient à l'une des classes α ou β. De (14) on déduit les équations correspondantes pour les conjugués; nous envisageons à présent seulement les équations correspondant aux indices des conjugués appartenant à la classe α. Nous formons le produit de toutes ces équations, γ comptant doublement une équation correspondant à un index α si $\mathfrak{I}^{(\alpha)}$ est un nombre complexe. Il résulte une équation entre les valeurs absolues des conjugués, et le côté droit ne contient aucun facteur excédant l'unité en valeur absolue. Le côté gauche sera > 1, parce que le produit contiendra pour chaque α le conjugué de ε_α qui excède 1, et l'on a déjà $\varepsilon^{(1)} \ldots \varepsilon^{(n)} = \pm 1$. L'indépendance des ε_i est donc établie.

Il y a un assez grand nombre de démonstrations du théorème de Dirichlet; je fais mention ici seulement d'une démonstration récente de v. d. Waerden [2], qui y introduit une forme nouvelle en évitant l'application des logarithmes et aussi du théorème de Minkowski. La démonstration précédente me semble avoir quelques mérites à cause de sa simplicité.

On connaît assez peu de propriétés des unités pour des corps généraux. Landau a montré l'existence dans chaque corps d'une unité η qui n'est pas une racine d'unité et qui satisfait les inégalités

$$|\log|\eta^{(a)}|| \leq \frac{1}{2^{n-1}(n-1)!}\,|\sqrt{|d|}\,|\,(\log|d|)^{n-1}$$

Wäisälä a donné des inégalités moins précises. Dans des travaux récents Remak [1], [2] a montré qu'on peut même trouver une limite supérieure M telle qu'il existe au moins un système fondamental pour lequel les valeurs absolues de tous les conjugués des unités n'excèdent pas M. On aura donc une méthode pour déterminer un système fondamental par un nombre fini d'opérations.

INDEX BIBLIOGRAPHIQUE.

Bauer (M.). — Ueber die Norm eines Ideals (*Abhandlungen math. Seminar Hamburg*, t. 5, 1927, p. 184).

Berwick (W. E. H.). — Integral bases (*Cambridge Tracts*, n° 22, 1927).

Cantor (G.). — Ueber eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen (*Journ. f. Mathematik*, t. 77, 1874, p. 258).

Dedekind (R.). — Œuvres complètes (Braunschweig, 1930).

Lejeune-Dirichlet (P. G.). — Vorlesungen über Zahlentheorie (4e édition, Braunschweig, 1894).

Furtwangler (P.). — 1. Ueber Kriterien für die algebraischen Zahlen (*Sitzungsber. d. Wiener Akad.*, 126 II *a*, 1917).

2. Zur Begründung der Idealtheorie (*Göttinger Nachrichten*, 1895, p. 381).

3. Punktgitter und Idealtheorie (*Math. Ann.*, t. 82, 1920, p. 256).

Gauss (C. F.). — Disquisitiones arithmeticæ.

Hasse (H.). — Ueber eindeutige Zerlegung in Primelemente oder in Primhauptideale in Integritätsbereichen (*Journ. f. Mathematik*, t. 159, 1928, p. 3).

Heawood (P. J.). — The classification of rational approximation (*Proc. London Math. Soc.*, 2e série, t. 20, 1921).

Hensel (K.). 1. Ueber die zu einem algebraischen Körper gehörigen Invarianten (*Journ. f. Mathematik*, t. 129, 1905, p. 68).

2. Ueber die Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor (*Journal f. Mathematik*, t. 103, 1888, p. 230).

3. Untersuchung der Zahlen eines algebraischen Körpers für den Bereich eines beliebigen Primteilers (*Journ. f. Mathematik*, t. 145, 1915, p. 92).

4. Die multiplikative Darstellung der algebraischen Zahlen für den Bereich eines beliebigen Primteilers (*Journ. f. Mathematik*, t. 146, 1916, p. 189).

5. Untersuchung der Zahlen eines algebraischen Körpers für eine beliebige Primteilerpotenz als Modul (*Journ. f. Mathematik*, t. 146, 1916, p. 216).

6. Allgemeine Theorie der Kongruenzklassengruppen und ihrer Invarianten in algebraischen Körpern (*Journ. f. Mathematik*, t. 147, 1917, p. 1).

7. Zur multiplikativen Darstellung der algebraischen Zahlen für den Bereich eines Primteilers (*Journ. f. Mathematik*, t. 151, 1921, p. 210).

HERMITE (Ch.). — Extrait d'une lettre de M. Ch. Hermite à H. Borckhardt, etc. (*Journ. f. Mathematik*, t. 53, 1857, p. 182).

HILBERT (D.). — Ueber die Zerlegung der Ideale eines Zahlkörpers in Primideale (*Math. Ann.*, t. 44, 1894, p. 1).

HURWITZ (A.). — 1. Ueber die angenäherte Darstellung der Irrationalzahlen durch rationale Brüche (*Math. Ann.*, t. 39, 1891, p. 279).

2. Ueber die Theorie der Ideale (*Göttinger Nachrichten*, 1894, p. 291).

3. Zur Theorie der algebraischen Zahlen (*Göttinger Nachrichten*, 1895, p. 324).

4. Der Euklidsche Divisionssatz in einem endlichen algebraischen Zahl körper (*Math. Zeitschr.*, t 3, 1919, p. 123).

JACOBI (C. G. J.). — Allgemeine Theorie der Kettenbruchähnlichen Algo rithmen, etc. (*Journ. f. Mathematik*, t. 69, 1868, p. 29).

KRONECKER (L.). — Zwei Sätze über Gleichungen mit ganzzahligen Koeffi zienten (*Œuvres*, t. 1, p. 103).

LANDAU (E.). — Abschätzungen von Charaktersummen, Einheiten und Klassenzahlen (*Göttinger Nachrichten*, 1918, p. 19).

LIOUVILLE (J.). — Sur des classes très étendues de quantités, etc. (*Journ. de Math.*, 1re série, t. 16, 1851, p. 133).

MAILLET (E.). — Introduction à la théorie des nombres transcendants et des propriétés arithmétiques des fonctions (Paris, 1906).

MINKOWSKI (H.). — 1. Ein Kriterium für die algebraischen Zahlen (*Göttinger Nachrichten*, 1899).

2. Ueber periodische Approximationen algebraischer Zahlen (*Acta Mathematica*, t. 26, 1902, p. 333).

3. Diophantische Approximationen (Leipzig, 1907).

4. Zur Theorie der Einheiten in den algebraischen Zahlkörpern (*Göttinger Nachrichten*, 1900, p. 90).

MOORE (E. H.). — A doubly infinite system of simple groups (*Bulletin New-York Math. Soc.*, t. 3, 1894, p. 73).

ORE (O.). — 1. Ueber die arithmetischen Eigenschaften gewisser Reihen. Académie des Sciences (Oslo, 1925).

2. Problème (*Jahresbericht d. Deutschen Math. ver.*, t. 39, 1930, p. 1; *voir* aussi Solutions, p. 9).

3. Einige Untersuchungen ueber endliche Körper (*VIIe Congrès des Mathématiciens scandinaves*, Oslo, 1930, p. 65).

PERRON (O.). — 1. Ueber die Approximation irrationaler Zahlen durch rationale I, II (*Sitzungsber. Heidelberger Akademie*, 1921).

2. Grundlagen einer Theorie des Jacobischen Kettenbruchalgorithmus (*Math. Ann.*, t. 64, 1907, p. 1).

PIPPING (N.). — Ein Kriterium für die reellen algebraischen Zahlen auf eine direkte Verallgemeinerung des Euklischen Algorithmus gegründet (*Acta Acad. Aboensis*, t. 1, 1922).

REMAK (R.). — 1. Elementare Abschätzungen von Fundamentaleinheiten und des Regulators eines algebraischen Zahlkörpers (*Journ. f. Mathematik*, t. 165, 1931, p. 159).

2. Ueber die Abschätzung des absoluten Betrages des Regulators eines algebraischen Zahlkörpers nach unten (*Journ. f. Mathematik*, t. 167, 1932, p. 360).

SIEGEL (C.). — Approximationen algebraischer Zahlen (*Math. Zeitschr.*, t. 10, 1921, p. 173).

TAKENOUCHI (T.). — On the classes of congruent integers in an algebraic Körper (*Journal, College of Science Tokyo*, t. 36, 1913).

THUE (A.). Ueber Annäherungswerte algebraischer Zahlen (*Journ. f. Mathematik*, t. 135, 1909, p. 284).

WAERDEN (B. v. d.). — 1. Ein logarithmenfreier Beweis des Dirichletschen Einheitensatzes (*Abhandlungen, Math. Sem. Hamburg*, t. 6, 1928, p. 259).

2. Moderne Algebra, Berlin, 1931.

WAISALA (R.). — Abschätzungen der Einheiten eines gegebenen algebraischen Körpers. (*Ofversikt Finska Vet. soc. förh. Helsingfors*, t. 61, 1918, n° 13).

WESTLUND (J.). — Primitive roots of ideals in algebraic numberfields (*Math. Ann.*, t. 11, 1912, p. 246).

WIMAN (A.). — Ueber die Ideale in einem algebraischen Zahlkörper, nach denen Primitivzahlen existieren (*Ofversikt Svenska Vet. akad. förh.*, t. 56, 1899).

WOLFF (G.). — Ueber die Gruppen der Reste eines beliebigen Moduls im allgebraischen Zahlkörper (*Thèse*, Giessen, 1905).

TABLE DES MATIÈRES.

92699 34. Paris. Imprimerie GAUTHIER-VILLARS, quai des Grands Augustins, 55.