

# BIBLIOGRAPHIE DE L'ARITHMÉTIQUE

Autor(en): **Chatelet, Albert**

Objektyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **8 (1962)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **20.09.2024**

Persistenter Link: <https://doi.org/10.5169/seals-37965>

## **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern. Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden. Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

## **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

# BIBLIOGRAPHIE DE L'ARITHMÉTIQUE <sup>1)</sup>

par Albert CHATELET

Cette conférence a pour but de présenter une liste d'ouvrages sur la théorie des nombres et l'arithmétique. Ils ont été classés et commentés suivant une division nécessairement assez arbitraire. L'ordre choisi est à peu près l'ordre chronologique d'apparition des différentes théories; mais le développement de chacune de ces théories a été envisagé séparément. Il y a malheureusement peu d'ouvrages récents écrits en français.

## 1. NOMBRES REMARQUABLES — FIGURES MAGIQUES

L'arithmétique a existé en Grèce en même temps que la géométrie et les progrès de ces 2 branches des mathématiques ont été en relations constantes.

Les Pythagoriciens ont étudié les propriétés des nombres remarquables: nombres carrés, triangulaires, cubes, polygonaux, nombres parfaits (égaux à la somme de leurs diviseurs), nombres amis (chacun d'entre eux égal à la somme des diviseurs de l'autre).

On peut rattacher à cet ordre de considérations:

Les expressions et formules *d'analyse combinatoire*:

Les *partitions* de nombres et la représentation des nombres par des sommes.

*Les figures magiques.*

Les problèmes de *jeux* (échecs, cartes, ...).

Ces problèmes ont été abordés par de nombreux chercheurs isolés et rarement rattachés à des théories générales.

Bibliographie: 12, 15, 30, 37.

---

<sup>1)</sup> Cette conférence a été prononcée en avril 1943 devant le séminaire d'algèbre et de théorie des nombres de la Faculté des Sciences de Paris. Nous la publions sans changement mais la liste d'ouvrages a été profondément modifiée pour tenir compte des nombreux ouvrages parus depuis cette date. La nouvelle liste a été établie grâce à la collaboration de MM. Chabauty, Descombes, Poitou et Néron.

2. DIVISIBILITÉ DES ENTIERS ORDINAIRES  
ET DES ENTIERS ALGÈBRIQUES

La géométrie d'Euclide expose la *théorie de la divisibilité*: algorithme d'Euclide, propriétés du p.g.c.d. et du p.p.c.m. décomposition des nombres en produits de facteurs premiers.

On peut rattacher, à ces préoccupations, les extensions de la théorie de la divisibilité à des ensembles où existent, une addition (commutative et associative), une soustraction, une multiplication (commutative, associative et distributive), appelés *anneaux*.

Un premier type de ces extensions est l'étude des *polynômes d'une variable* dont les coefficients sont dans un corps. Il existe des polynômes irréductibles, jouant la rôle de facteurs premiers, mais leur définition n'est pas absolue, elle dépend du corps. Les coefficients jouent le rôle de diviseurs de 1.

Un autre type d'extension est l'ensemble des *entiers de Gauss*  $a+bi$ , avec  $a$  et  $b$  entiers rationnels. Il y a cette fois 4 nombres  $\pm 1, \pm i$  qui jouent le rôle de diviseurs de 1, c'est-à-dire qui ont des inverses. On ne distingue pas les nombres qui ne diffèrent entre eux que par multiplication par un de ces diviseurs de 1. Il existe encore un algorithme de division et une décomposition des entiers en facteurs premiers. Ces propriétés établissent en même temps celles des entiers qui peuvent être représentés par une somme de 2 carrés, grâce à la relation  $a^2+b^2 = (a+bi)(a-bi)$ .

Pour l'étude du problème de Fermat, on a tenté de généraliser ces propriétés aux entiers de la *division du cercle*, correspondant à la décomposition  $a^n+b^n = \Pi(a+b\omega_i)$ . KUMMER a montré qu'il n'y a plus nécessairement une décomposition en facteurs premiers et en a déduit la nécessité d'introduire des *facteurs idéaux*.

Des exemples plus généraux ont été envisagés: entiers algébriques, racines d'équation de la forme  $x^n+a_1x^{n-1}+\dots=0$ ,  $a_i$  entiers ordinaires. Le point de vue de KUMMER a été repris pour des entiers algébriques par DEDEKIND, qui a interprété le facteur idéal par un ensemble convenable de tels entiers.

Bibliographie: 1, 7, 9, 12, 15, 20, 30, 36, 37.

### 3. ANALYSE INDÉTERMINÉE DU PREMIER DEGRÉ

L'arithmétique de Diophante a introduit un symbolisme algébrique et l'usage d'équations. La résolution de ces équations était dominée par la préoccupation de *tomber juste*.

Ce traité a eu une longue influence sur le développement des mathématiques, grâce à l'édition de BACHET DE MEZIRIAC (1621); cet auteur a également publié un ouvrage personnel consacré à des questions analogues: Problèmes plaisants et délectables qui se font par les nombres. Quelques années plus tard (1670), le fils de Pierre de FERMAT publiait les annotations transcrites dans les marges d'un exemplaire de l'Arithmétique de Diophante par son père; elles comportaient des énoncés de propriétés nouvelles et parfois des solutions de problèmes.

Quoiqu'il en soit, on appelle *problèmes diophantiens* (ou diophantiques) la recherche des solutions en nombres entiers ou en nombres rationnels des équations à coefficients entiers ou rationnels.

On appelle aussi l'ensemble de ces problèmes *analyse indéterminée*.

Le cas d'une équation, ou d'un système d'équations, du premier degré est presque complètement résolu.

L'étude de  $ax+by=c$ ,  $a, b, c$ , entiers donnés,  $x, y$  entiers inconnus, est liée à la divisibilité, mais aussi à l'ensemble des nombres de la forme  $ax+by$ , qui sont des multiples du p.g.c.d. de  $a$  et  $b$ . On peut aussi interpréter l'étude de ce dernier ensemble par celle des *réseaux de points*, ce qui conduit aux *fractions continues* et aux *substitutions unimodulaires*. Ces questions ont été abordées par BACHET, FERMAT, EULER, LAGRANGE.

L'étude des systèmes d'équations peut être faite par des méthodes analogues; elle a été développée par Gauss, Poincaré, Smith, Frobenius, Heger.

Bibliographie: 7, 8, 9, 12, 41.

### 4. EQUATIONS DIOPHANTIENNES DE DEGRÉ SUPÉRIEUR

Les équations diophantiennes de degré supérieur sont de types très divers; par exemple (équations non homogènes):

$$p = x^2 + y^2; \quad x^2 - dy^2 = 1; \quad x^2 + y^2 + z^2 + t^2 = 1$$

ou (équations homogènes):

$$x^2 + y^2 = z^2, \quad y^2 z - x^3 = 0, \dots$$

Une première catégorie de problèmes est la recherche des *points à coordonnées entières*, ou à *coordonnées rationnelles* (en abrégé points entiers, ou points rationnels) sur des courbes algébriques à coefficients entiers.

Par exemple: recherche de  $x, y, z$  entiers tels que:

$$x^2 + y^2 = z^2$$

(points rationnels sur un cercle);  $x/y = t$  est rationnel et  $x/z, y/z$  s'en déduisent par les formules:

$$\frac{x}{z} = \frac{1 - t^2}{1 + t^2} \quad \frac{y}{z} = \frac{2t}{1 + t^2}$$

ou encore  $x, y, z$  sont proportionnels à

$$\lambda^2 - \rho^2, \quad 2\lambda\rho, \quad \lambda^2 + \rho^2$$

avec  $\lambda, \rho$  entiers premiers entre eux.

Plus généralement, on peut chercher les points entiers, ou les points rationnels, sur des *surfaces*, ou sur des *variétés algébriques* déterminées par des relations à coefficients entiers.

Ces problèmes ont donné lieu à de nombreuses recherches dispersées et à des solutions de fortune, notamment de FERMAT, EULER, LAGRANGE. Des recherches plus systématiques ont été entreprises dans ces dernières années, surtout par H. POINCARÉ et A. WEIL.

Bibliographie: 4, 12, 15, 23, 29, 33, 38, 41.

## 5. CONGRUENCES ET CORPS FINIS

L'étude du problème de Fermat ont conduit EULER, LAGRANGE, LEGENDRE, JACOBI à établir une théorie qui a été mise au point par GAUSS. Elle a été exposée dans les *Disquisitiones arithmeticae* parus en latin en 1801 et traduite depuis en français.

Cette théorie étudie l'arithmétique et l'algèbre des entiers définis à l'addition près d'un multiple d'un entier fixe  $p$ ; les relations obtenues sont appelées *congruences* suivant le module  $p$ . Les entiers, ainsi définis, ne déterminent qu'un nombre fini d'êtres, encore appelées classes de congruence.

Si l'entier  $p$  (caractéristique) est premier, l'ensemble des classes forme un corps, c'est-à-dire que les 4 opérations élémentaires sont possibles. Mais le polynome  $x^{p-1} - 1$  est nul pour toute valeur  $x$  du corps, sans être identiquement nul; plus généralement un polynome  $F(x^p)$  peut être irréductible et n'avoir que des racines multiples.

Dans une note assez brève, E. GALOIS complète ces résultats par l'introduction d'imaginaires. Il considère des êtres  $f(i)$ , définis suivant 2 modules  $p$  et  $\varphi(i)$ , où  $\varphi$  est un polynome irréductible de degré  $f$ . Il obtient ainsi  $p^f$  êtres, ou imaginaires de Galois; toute équation de degré  $f$  à coefficients rationnels est décomposable.

DICKSON a montré que les ensembles d'imaginaires de Galois forment tous les *corps* qui ne contiennent qu'un *nombre fini d'éléments* (corps finis). L'étude de ces corps est indispensable pour la résolution des équations diophantiennes.

HENSEL a introduit des corps (infinis) — les corps locaux ou  $p$ -adiques — qui permettent d'utiliser les propriétés des congruences suivant les modules puissances de nombres premiers. Un tel corps est constitué par les séries formelles  $(a_0 + a_1p + \dots)$ , où les  $a_i$  sont des entiers définis au module  $p$  près.

Bibliographie: 2, 3, 9, 12, 13, 14, 15, 18, 27, 30, 37.

## 6. FORMES QUADRATIQUES

L'équation congruentielle:

$$x^2 - q \equiv 0 \pmod{p}$$

a été particulièrement étudiée à 2 points de vue différents:  $p$  étant donné, trouver les  $q$  (appelés restes quadratiques mod.  $p$ );  $q$  étant donné, trouver les  $p$ .

La loi de réciprocité quadratique de GAUSS lie ces 2 points de vue.

Mais les diviseurs  $p$  de  $x^2 - q$  sont les mêmes que ceux de  $x^2 - qy^2$  (si ces diviseurs  $p$  sont sans facteurs carrés et premiers à  $q$ ); cette dernière expression est un cas particulier d'une *forme quadratique binaire*

$$ax^2 + bxy + cy^2.$$

L'étude des formes quadratiques binaires a été débutée par GAUSS et continuée par HERMITE. On appelle formes *équivalentes* celles qui représentent les mêmes nombres; elles peuvent être déduites les unes des autres par des substitutions unimodulaires. Dans chaque classe de formes équivalentes, on cherche des formes *réduites*. Ces problèmes sont liés, en analyse, à l'étude des fonctions fuchsiennes.

L'étude des formes quadratiques à 3, 4, ... variables a donné lieu à de nombreux travaux, mais pose encore des problèmes importants. L'étude des formes de degré supérieur est seulement ébauchée.

L'étude des formes quadratiques binaires a été partiellement abandonnée et remplacée par celle des corps quadratiques, grâce à la relation:

$$ax^2 + bxy + cy^2 = (\alpha x + \beta y)(\alpha' x + \beta' y)$$

avec  $\alpha, \beta$  nombres quadratiques.

Bibliographie: 15, 18, 21, 30, 34, 43.

## 7. APPROXIMATIONS DIOPHANTIENNES

Etant donné un nombre rationnel ou irrationnel, on peut chercher les fractions rationnelles à termes simples qui en diffèrent peu; c'est le problème des approximations diophantiennes.

La seule solution entièrement satisfaisante est celle des *fractions continues*. Il est remarquable qu'elle soit liée à la théorie des formes quadratiques binaires, du développement périodique des irrationnelles du second degré et aux substitutions unimodulaires.

Ces théories ont été reprises et généralisées d'un point de vue géométrique très simple par MINKOWSKI. Cette méthode conduit à des *théorèmes d'existence* en théorie des nombres.

On peut rattacher à ces questions la démonstration de la *transcendance* des nombres  $e$  et  $\pi$  par HERMITE et LINDEMANN. SIEGEL a aussi démontré la transcendance d'autres nombres.

Bibliographie: 5, 6, 11, 15, 22, 23, 24, 29, 30, 31, 32, 38, 39, 40, 42.

## 8. LES NOMBRES PREMIERS

Les nombres premiers forment la base minimum permettant d'engendrer le groupe multiplicatif des entiers:  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots$ . Ce fait a pour conséquence une propriété des séries:

$$\prod \left( \frac{1}{1 - \frac{1}{p^s}} \right) = \sum \frac{1}{n^s}$$

Cette série ne converge que pour  $s > 1$ ; mais la série:

$$\frac{1}{1 - \frac{1}{p^s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots$$

converge pour  $s \geq 1$ .

La divergence de la série  $\sum \frac{1}{n^s}$  pour  $s = 1$  a notamment pour conséquence l'existence d'une *infinité de nombres premiers*. L'étude de cette série, appelée  $\zeta(s)$ , a fourni plus généralement des renseignements sur la répartition des nombres premiers. On peut y rattacher les études sur les séries de DIRICHLET, les études de HADAMARD sur les fonctions entières, notamment la définition du genre et les études de la VALLÉE POUSSION.

La méthode précédente pour démontrer l'existence d'une infinité de nombres premiers peut être généralisée. Par exemple, en désignant par  $p$  les nombres premiers égaux à la somme de 1



et d'un multiple de 4 et par  $q$  les nombres premiers égaux à la différence d'un multiple de 4 et de 1, on obtient :

$$\prod \left( \frac{1}{1 - \frac{1}{p^s}} \right) \prod \left( \frac{1}{1 - \frac{1}{q^{2s}}} \right) = \sum \frac{1}{m^s}$$

où  $m$  décrit tous les entiers impairs décomposables en une somme de 2 carrés ( $a^2 + b^2$ ). La divergence de la série pour  $s = 1$  entraîne l'existence d'une infinité de nombres premiers de la forme  $p$  et de la forme  $q$ . Plus généralement LEJEUNE-DIRICHLET a démontré l'existence d'une infinité de nombres premiers dans toute *progression arithmétique* dont la raison et le premier terme sont premiers entre eux.

HECKE a étudié de façon analogue les nombres premiers qui sont normes d'idéaux d'un corps de nombres algébriques donné.

Bibliographie: 11, 15, 18, 19, 23, 27, 28, 30, 38.

## 9. THÉORIE DES GROUPES ET SUBSTITUTIONS

La notion de groupe est apparue dans l'étude des permutations d'un nombre fini d'éléments, et plus particulièrement dans l'étude des permutations entre différentes racines d'une même équation algébrique.

On peut faire remonter l'origine de cette notion et de ces méthodes à PASCAL, NEWTON, et surtout VANDERMONDE, dans leurs recherches sur les équations binomes et la construction des polygones. Mais c'est LAGRANGE et ABEL qui les ont clairement dégagées pour les équations abéliennes et GALOIS pour le cas général. JORDAN a repris les méthodes de GALOIS et les a exposées magistralement.

SOPHUS LIE, Elie CARTAN ont généralisé ces méthodes à des opérations sur des fonctions.

Plus récemment a été introduite une définition abstraite des groupes et ont été étudiées les propriétés de ces ensembles.

Bibliographie: 8, 9, 13, 20, 25, 36, 44.

## 10. LES ÉQUATIONS ET LES CORPS ALGÈBRIQUES

La théorie des équations conduit à la notion d'*extension* ou de *corps de nombres algébriques*.

On considère l'ensemble des nombres rationnels  $R$  et une équation irréductible:

$$\varphi(x) = 0$$

à coefficients dans  $R$ . L'ensemble des polynômes  $f(x)$  à coefficients dans  $R$ , définis au module  $\varphi(x)$  près, est un corps: les 4 opérations élémentaires sont possibles pour les éléments de cet ensemble. Tout se passe encore comme si on ajoutait à  $R$  une irrationnelle  $\alpha$ , racine de l'équation considérée; on dit que ce corps est l'*extension*  $R(\alpha)$  de  $R$  par  $\alpha$ .

Si  $\alpha_1, \alpha_2 \dots \alpha_n$  sont les différentes racines de l'équation

$$\varphi(x) = 0$$

on peut construire les extensions:

$$R(\alpha_1), \quad R(\alpha_2), \dots, R(\alpha_n).$$

Ces corps sont isomorphes, c'est-à-dire que l'on passe de l'un à l'autre par une substitution qui conserve les 4 opérations élémentaires et qui laisse invariants les éléments de  $R$ .

Plus généralement, on peut construire des *extensions algébriques finies*, en faisant successivement plusieurs extensions par adjonction d'une racine d'une équation à coefficients dans le corps déjà formé.

Ce point de vue s'est dégagé progressivement dans la seconde moitié du XIX<sup>e</sup> siècle.

Bibliographie: 1, 2, 7, 9, 13, 15, 17, 18, 19, 20, 30, 36, 44, 45, 46.

## 11. PROPRIÉTÉS ARITHMÉTIQUES DE CORPS ALGÈBRIQUES

Il a déjà été dit qu'on peut étendre aux corps algébriques la notion d'*entiers* et de *divisibilité* entre entiers, ce qui conduit à la construction des *idéaux*.

On peut aussi chercher des relations arithmétiques entre plusieurs corps algébriques; le point de départ de ces études semble être la loi de réciprocité quadratique de Legendre et Gauss.

On étudie la possibilité de solutions en entiers  $x$  (ou  $y$ ) des congruences :

$$x^2 - q \equiv 0 \pmod{p}$$

$$y^2 - p \equiv 0 \pmod{p}$$

ou  $p$  et  $q$  sont 2 nombres premiers (positifs). La loi de réciprocité quadratique établit un lien entre ces 2 congruences: si l'un des nombres premiers  $p$  ou  $q$  est de la forme  $4n+1$ , avec  $n$  entier, ces 2 congruences sont simultanément possibles ou impossibles; si aucun des nombres  $p$  et  $q$  n'est de la forme  $4n+1$ , la possibilité d'une des congruences exclut celle de l'autre.

Or la possibilité de la congruence :

$$x^2 - q \equiv 0 \pmod{p}$$

peut être interprétée comme une condition nécessaire et suffisante pour que le nombre premier  $p$  soit décomposé en un produit de 2 idéaux premiers dans le corps quadratique engendré par  $\sqrt{q}$ . La loi de réciprocité quadratique établit ainsi un lien entre l'arithmétique dans les 2 corps quadratiques engendrés respectivement par  $\sqrt{p}$  et  $\sqrt{q}$ .

On peut d'ailleurs démontrer cette loi en construisant le corps de  $\sqrt{q}$  au moyen de racines  $q$ èmes de l'unité. L'idée de cette démonstration provient de recherches de GAUSS sur la construction des polygones réguliers. Cette démonstration introduit un lien entre l'arithmétique du corps des racines  $q$ èmes de l'unité et du corps quadratique engendré par  $\sqrt{p}$ .

D'autres lois de réciprocité ont pu être démontrées et rassemblées dans la *théorie du corps des classes*.

Bibliographie: 1, 10, 17, 19, 20, 26, 27, 46.

## 12. NOTION GÉNÉRALE D'IDÉAUX

L'extension d'un corps par un nombre algébrique a conduit à introduire d'autres extensions et à les définir d'un point de vue plus axiomatique. La notion d'*anneau* est ainsi apparue importante:

ensemble qui forme un groupe pour une opération d'addition et dans lequel est définie une opération de multiplication. Dans un anneau, un *idéal* est un ensemble qui contient la somme et la différence de 2 quelconques de ses éléments, ainsi que le produit d'un de ses éléments par un élément quelconque de l'anneau.

L'intérêt de ces notions est de permettre des raisonnements généraux applicables à des cas particuliers très différents. Par exemple: arithmétique dans un corps de nombres algébriques, géométrie des *variétés algébriques*, ...

A ces propriétés, on peut rattacher les études sur les *matrices*.

Bibliographie: 8, 9, 10, 17, 25, 35, 46.

## BIBLIOGRAPHIE

1. E. ARTIN, Gottingen 1959.

Theory of algebraic numbers.

Cours professé à l'Université de Gottingen.

Exposé des notions et résultats classiques de la théorie des nombres algébriques: entiers, idéaux, unités, classes d'idéaux; cet exposé utilise méthodiquement la théorie des valuations.

2. E. BOREL et J. DRACH, Vuibert 1894.

Introduction à l'étude de la théorie des nombres et de l'algèbre supérieure, d'après les conférences de J. TANNERY. Ouvrage ancien, mais qui reste une bonne introduction à l'étude des congruences, des imaginaires de Galois et des corps de nombres algébriques.

3. D. CARMICHÆL, Presses universitaires 1929.

Théorie des nombres. Traduction par A. SALLIN.

Notice très sommaire sur l'indicateur, les congruences, le théorème de Fermat et les racines primitives. Nombreux exercices.

4. D. CARMICHÆL, Presses universitaires 1929.

Analyse indéterminée. Traduction par A. SALLIN.

Equations à résoudre en nombres entiers. Triangles ration-

nels. Equations du 2<sup>e</sup> et du 3<sup>e</sup> degré. Dernier théorème de Fermat. Equations fonctionnelles.

5. J. W. S. CASSELS, Cambridge 1957.

An introduction to diophantine approximation.

Exposé analogue à celui de Koksma (24) sur le même sujet, et rendant compte des progrès accomplis de 1936 à 1956.

Approximation de zéro par une forme linéaire, homogène ou non, à coefficients irrationnels et à variables entières; approximation simultanée de zéro par plusieurs formes analogues. Théorème de Thue — Siegel — Roth sur l'approximation des nombres algébriques.

6. J. W. S. CASSELS, Berlin 1959.

An introduction to the geometry of numbers.

Exposé moderne de la théorie fondée par Minkowski. (Cf. Minkowski, 33).

7. A. CHATELET, Gauthiers Villars 1913.

Leçons sur la théorie des nombres.

Algèbre des matrices permutables. Modules ou réseaux de points. Equations et formes linéaires à coefficients entiers. Nombres et entiers algébriques, divisibilité, idéaux, réduction continue, unités, classes d'idéaux. Notes sur les fonctions quasi-périodiques, sur un corps quadratique, sur les normes des idéaux.

8. A. CHATELET, Gauthiers Villars 1925.

Les groupes abéliens finis et les modules de points entiers. Modules (ou idéaux) de points entiers, arithmétique des matrices. Groupes abéliens, automorphismes, caractères, sous-groupes, sous-groupes caractéristiques. Composition des groupes. Diviseurs d'un produit direct. Quelques notes bibliographiques.

9. A. CHATELET, Presses universitaires 1954-1956.

Arithmétique et algèbre modernes.

Tome I. Notions fondamentales: notations, ensembles, treillis d'ensembles, correspondances, opérations. Groupes:

propriétés caractéristiques, sous-groupes, groupes de transformations, treillis de sous-groupes, modules de points entiers, fonctions arithmétiques, sous-groupes d'ordre fini. Tome II. Anneaux et corps: décomposition d'un anneau, anneaux d'endomorphismes d'un module, décomposition d'un module en somme directe, corps. Calcul algébrique: polynomes, opérations bilinéaires, matrices. Idéaux et divisibilité: propriétés des idéaux, anneaux d'Artin, anneaux noëthériens, décomposition des idéaux d'un anneau. Tome III (à paraître): Idéaux d'un domaine d'intégrité. Espaces linéaires sur un corps et sur un domaine d'intégrité. Extensions finies d'un corps.

10. C. CHEVALLEY, Nagoya 1954.

Class field theory.

Exposé de la théorie du corps des classes utilisant les méthodes d'algèbre homologique.

11. COLLOQUE DU CENTRE BELGE DE RECHERCHES MATHÉMATIQUES, Masson 1956.

La théorie des nombres.

Exposé de questions diverses de théorie additive des nombres, d'arithmétique analytique, et de problèmes d'approximation diophantienne. On y trouve en particulier une démonstration par l'auteur du théorème de Roth sur l'approximation des nombres algébriques.

12. L. E. DICKSON, Londres 1919-20-23.

History of the theory of numbers.

Analyse sommaire de très nombreuses publications sur la théorie élémentaire des nombres (congruences, divisibilité). Tables numériques. Equations diophantiennes linéaires et de degré supérieur.

13. E. GALOIS, Gauthiers Villars 1897.

Œuvres mathématiques.

Sous une forme concise contiennent les notions essentielles de la théorie des groupes: isomorphisme, sous groupes,

suite de composition et leur application à la résolubilité des équations par radicaux. Un court article sur la théorie des nombres contient la définition des « imaginaires de Galois ».

14. K. F. GAUSS, Blanchard 1807 et 1953.

Recherches arithmétiques; traduction de POULLET DELISLE. C'est l'origine de la théorie des congruences et des formes quadratiques.

15. C. H. HARDY et E. M. WRIGHT, Oxford 1961.

An introduction to the theory of numbers.

Nombres premiers. Suite de Farey et théorème d'approximation des nombres irrationnels de Minkowski. Congruences et résidus. Fractions continues et approximations. Entiers de Gauss. Corps quadratiques. Fonctions arithmétiques. Partition des nombres. Représentation des nombres par des sommes de carrés ou de cubes. Densité des nombres premiers. Compléments sur les approximations des nombres.

16. C. H. HARDY et E. M. WRIGHT, Munich 1958.

Einführung in die Zahlentheorie.

C'est la traduction en langue allemande de l'ouvrage précédent.

17. H. HASSE, Berlin 1949.

Zahlentheorie.

Exposé de la théorie des corps de nombres algébriques utilisant les propriétés des corps valués et les analogies avec la théorie des corps de fonctions algébriques.

18. H. HASSE, Berlin 1950.

Vorlesungen über Zahlentheorie.

Exposé classique sur les restes quadratiques, le théorème de Dirichlet sur les nombres premiers, les corps quadratiques.

19. E. HECKE, Leipzig 1923 et Chelsea 1948.

Vorlesungen über die Theorie der algebraischen Zahlen. Exposé classique sur la théorie des corps de nombres algé-

briques et sur l'arithmétique de leurs entiers. Démonstration de la loi de réciprocité quadratique dans un corps de nombres algébriques.

20. J. HERBRAND, Gauthiers Villars 1936.

Le développement moderne de la théorie des corps algébriques.

Un résumé très net de la théorie générale des corps algébriques. Exposé de la théorie de classes et des lois de réciprocité, suivant les travaux de Hilbert, Takagi, Artin.

21. B. W. JONES, Wiley 1950.

Arithmetical theory of quadratic formes.

Etudes des formes quadratiques dans le corps des réels, les corps  $p$ -adiques, le corps des nombres rationnels, dans un anneau des entiers  $p$ -adiques, dans l'anneau des entiers rationnels.

Relations avec la théorie des idéaux dans un corps de nombres quadratiques.

22. O. KELLER, Teubner 1954.

Geometrie der Zahlen.

Exposé récent et condensé de la théorie fondée par Minkowski. (Cf. Minkowski, 33).

23. A. Y. KINCHIN, Graylock Press Rochester 1952.

Three pearls of number theory.

Theorème de Van der Waerden sur les progressions arithmétiques. Hypothèse de Landau Schnirelmann. Solution élémentaire du problème de Waring.

24. J. F. KOKSMA, Springer 1936.

Diophantische Approximationen.

Exposé des résultats récents sur les approximations des nombres irrationnels par des fractions. Géométrie des nombres. Cas linéaire homogène et cas non homogène. Fractions continues.



25. W. KRULL, Springer 1935.  
Idealtheorie.  
Exposé des résultats essentiels de la théorie des idéaux.  
Théorèmes de décomposition. Anneaux de polynômes.  
Théorie des valeurs absolues.  
Idéaux de Prüfer.
26. E. LANDAU, Chelsea 1949.  
Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale.  
Exposé centré sur les fonctions Zêta des corps de nombres algébriques; équation fonctionnelle, zéros, application à la répartition des idéaux premiers.
27. E. LANDAU, Chelsea 1946.  
Vorlesungen über Zahlentheorie.  
I. 1—Elementare Zahlentheorie  
Congruences, restes quadratiques, équation de Pell, nombres premiers dans une progression arithmétique, somme de 2, 3, 4 carrés, formes quadratiques binaires.  
I. 2—Hypothèse de Goldbach, problème de Waring.  
II. Etude approfondie, par les moyens analytiques, de la répartition des nombres premiers.  
III. Théorie des nombres algébriques et problème de Fermat.
28. E. LANDAU, Chelsea 1953.  
Handbuch der Lehre von der Verteilung der Primzahlen.  
Exposé systématique, le premier en date et très détaillé, de la théorie analytique des nombres premiers: répartition dans une progression arithmétique et applications, séries de Dirichlet.
29. E. LANDAU, Berlin 1959.  
Diophantische Gleichungen mit endlich vielen Lösungen.  
Nouvel exposé d'un chapitre du livre précédent de Landau 27, tome III, par A. Walfisz. Ce chapitre était consacré aux théorèmes de Thue et de Siegel sur la résolution en

nombres entiers de certaines équations indéterminées. Le nouvel exposé complète ces théorèmes par le récent théorème de Roth.

30. W. LEVEQUE, Add. Wesley 1956.

Topics in number theory (2 vol.).

Ce cours commence l'exposé de la théorie des nombres à un niveau très élémentaire, puis traite en particulier les questions suivantes: congruences; résidus quadratiques; fonctions arithmétiques et répartition des nombres premiers; sommes de carrés; formes quadratiques définies et indéfinies; corps de nombres algébriques; approximation des nombres algébriques par des rationnels; problèmes de transcendance.

31. H. MINKOWSKI, Chelsea 1953.

Geometrie der Zahlen.

Theorie méthodique des approximations par l'utilisation de corps convexes dans l'espace à  $n$  dimensions.

32. H. MINKOWSKI, Chelsea 1947.

Diophantische Approximationen.

Procédés géométriques appliqués à des recherches d'approximations de nombres. Application aux nombres algébriques. C'est un exposé élémentaire de l'ouvrage précédent.

33. T. NAGELL, Gauthiers Villars 1929.

L'analyse indéterminée de degré supérieur.

Exposé des résultats obtenus en 1929 sur la résolution en nombres entiers ou en nombres rationnels d'équations algébriques de degré supérieur à 1.

34. H. MAASS, S.V. 1949.

Automorphe Funktionen und indefinite quadratische Formen.

Théorie analytique des problèmes arithmétiques sur les formes quadratiques indéfinies.

35. D. G. NORTHCOTT, Cambridge University Press 1953.  
Ideal theory.  
Exposé succinct des propriétés des idéaux en relation avec la géométrie algébrique: idéaux dans les anneaux noethériens, anneaux locaux.
36. O. ORE, Gauthiers Villars 1934.  
Les corps algébriques et la théorie des idéaux.  
Exposé succinct sur la théorie des nombres algébriques. Corps. Entiers. Unités. Idéaux.
39. O. ORE, Mc Graw Hill 1948.  
Number theory and its history.  
Exposé simple sur la théorie élémentaire des nombres et sur son histoire.
38. H. OSTMANN, Springer 1956.  
Additive Zahlentheorie.  
Etude approfondie de la représentation d'un entier comme somme d'entiers satisfaisant à des conditions diverses. Le tome I contient les théories générales, le tome II traite notamment de la répartition des nombres premiers, du problème de Goldbach et du problème de Waring.
39. Th. SCHNEIDER, Gauthiers Villars 1959.  
Introduction aux nombres transcendants. Traduction de l'allemand.  
Exposé très complet des différentes méthodes d'étude des nombres transcendants. Travaux de Liouville, Hermite, Lindemann, Siegel, Mahler, Gelfond.
40. C. L. SIEGEL, Princeton 1959.  
Transcendental numbers.  
Au moyen de méthodes d'approximation, preuve de la transcendance de certains nombres: valeurs de fonctions spéciales (exponentielles, elliptiques) ou de solutions d'équations différentielles linéaires.

41. Th. SKOLEM, Gauthiers Villars 1938.  
Diophantische Gleichungen.  
Exposé des résultats sur la résolution des équations en nombres entiers ou rationnels. Equations linéaires. Equations quadratiques. Points rationnels sur une courbe algébrique. Points entiers sur une courbe algébrique.
42. I. M. VINOGRADOV, Interscience Publ. 1947.  
The method of trigonometrical sums in the theory of numbers.  
Exposé de la méthode d'estimation trouvée par l'auteur dans les années trente et applications: problème de Waring, répartition modulo un, problème de Goldbach.
43. G. L. WATSON, Cambridge 1960.  
Integral quadratic forms.  
Exposé élémentaire de la théorie des formes quadratiques à coefficients et variables entiers, centré sur les problèmes de l'équivalence, de la décomposition et de la représentation.
44. H. WEBER, 1895.  
Lehrbuch der Algebra.  
Tome I. Théorie des équations algébriques. Notions sur les corps et les domaines de rationalité.  
Tome II. Corps de nombres algébriques.  
Tome III. Fonctions elliptiques.
45. H. WEBER, Gauthiers Villars 1898.  
Traité d'algèbre supérieure.  
C'est la traduction française du tome I du livre précédent.
46. H. WEYL, Princeton 1957.  
Algebraic theory of numbers.  
Cours professé à l'Université de Princeton en 1938-39. Ce cours servait d'introduction à l'étude de la théorie du corps des classes; il développe les méthodes de Kronecker, Kummer, Hensel pour l'étude des idéaux.