NOTE II

chapitres précédents. Le livre récent de H. HASSE (*Zahlentheorie*, Berlin, 1959) contient un chapitre conçu dans le même esprit. Le livre plus élémentaire du même auteur (*Vorlesungen über Zahlentheorie*, Berlin, 1950) expose la théorie des corps quadratiques de façon plus détaillée et plus indépendante. D'autres traités (R. FUETER, *Synthetische Zahlentheorie*, Lepizig, 1919) utilisent plutôt les corps circulaires comme exemple de corps de nombres algébriques. Enfin certains (H. WEYL, *Algebraic theory of numbers*, Princeton, 1940; H. POLLARD, *The theory of algebraic numbers*, New York, 1950) ne consacrent que quelques lignes aux exemples particuliers de ces corps.

Une conférence d'Albert CHATELET (« L'arithmétique des idéaux », Conférences du Palais de la Découverte, Paris, 1950) étudie de façon détaillée et élémentaire deux exemples de corps quadratiques et compare l'arithmétique de leurs entiers et de leurs idéaux à celle des entiers rationnels.

Il faut enfin signaler que les exposés sur la théorie des formes quadratiques binaires sont essentiellement équivalents à un exposé sur l'arithmétique des corps quadratiques.

Le présent exposé précise et complète une méthode qui avait été esquissée par A. LÉVY au Congrès international de mathématiques réuni à Toronto (*Proc. Congress Toronto*, 1924, Tome 1, pp. 229-244). Cette méthode permet une construction effective du groupe des classes d'idéaux d'un corps quadratique, par des calculs élémentaires.

F. C.

NOTE II

La méthode utilisée ici, pour définir et construire un corps quadratique, a été choisie de telle sorte que les entiers (algébriques) du corps (**3**) puissent être engendrés de façon aussi simple que possible. C'est pour cette raison que l'entier caractéristique d est supposé dépourvu de facteurs carrés et que le polynome fondamental (**1**) se présente sous deux formes différentes, suivant que $d-1$ est ou n'est pas divisible par 4. Ce qui simplifie sensiblement l'exposé et les calculs ultérieurs.

Mais on peut se demander quelle est l'origine de la notion d'entier (d'un corps quadratique, ou plus généralement d'un corps de nombres algébriques de degré fini); ou encore se demander pourquoi les entiers ainsi définis ont une telle importance en arithmétique. On trouvera dans plusieurs ouvrages ou mémoires (notamment, dans l'article de R. DEDEKIND: « Sur la théorie des entiers algébriques », traduction française dans le *Bul. des Sc. math.*, 1876 et 1877) des explications sur l'origine et l'intérêt de la notion d'idéal dans l'anneau des entiers d'un corps algébrique. Mais, depuis GAUSS, la notion d'entier algébrique est rarement discutée.

On peut invoquer la propriété classique: tout élément d'une extension finie de l'anneau des entiers rationnels est entier algébrique (c'est-à-dire est zéro d'au moins un polynome d'une variable dont les coefficients sont des entiers rationnels et dont le coefficient de la puissance la plus élevée est 1). On trouvera la démonstration de cette propriété notamment dans le traité d'Albert CHATELET: *Arithmétique et Algèbre modernes*, Tome III (en préparation). La notion d'entier algébrique est essentiellement destinée à obtenir, entre ces entiers, des propriétés de divisibilité aussi analogues que possible à celle des entiers rationnels et comprenant ces dernières propriétés. Il est donc nécessaire que l'ensemble de ces nouveaux entiers contienne les entiers rationnels et les produits de nouveaux entiers par les entiers rationnels. Il est aussi souhaitable que l'ensemble des nouveaux entiers contienne la somme et la différence de 2 de ces éléments, comme l'ensemble des entiers rationnels contient une telle somme et une telle différence. Enfin, il est naturel de choisir, pour un corps de nombres algébriques donné, un ensemble de nombres du corps qui puissent être engendré, au moyen des opérations précédentes, à partir d'un ensemble restreint, si possible fini, de nouveaux entiers; et, s'il existe plusieurs ensembles vérifiant ces conditions, de choisir l'ensemble le plus étendu possible. Le résultat rappelé montre qu'il faut choisir l'ensemble de tous les entiers algébriques contenu dans le corps.

On peut aussi donner des explications moins axiomatiques et plus constructives, en discutant simultanément la notion d'entier et celle d'idéal. Lorsque GAUSS a introduit les extensions

du corps des nombres rationnels et de l'anneau des entiers rationnels par adjonction de l'imaginaire principale (corps de GAUSS et entiers de GAUSS), il cherchait à utiliser certains nombres algébriques pour résoudre des problèmes sur les entiers rationnels, et plus précisément des problèmes diophantiens. C'était une sorte de généralisation de la méthode de Jérôme CARDAN, qui avait utilisé des nombres imaginaires pour calculer les racines réelles d'une équation du troisième degré.

Ainsi, la recherche des systèmes d'entiers rationnels x, y, z qui vérifient la relation:

$$x^2 - ay^2 = bz^2, \tag{1}$$

où a, b, c sont des entiers donnés, peut être remplacée par la recherche des nombres algébriques conjugués, $\alpha = x + \sqrt{a}y$, $\alpha = x - \sqrt{a}y$, x, y entiers, qui vérifient la relation:

$$\alpha\bar{\alpha} = bz^2 \tag{2}$$

On peut chercher des propriétés de divisibilité entre les nombres algébriques, α, $\bar{\alpha}$, afin d'utiliser une méthode analoque à la méthode élémentaire de résolution d'une équation:

$$uv = bz^2.$$

Mais on peut aussi utiliser les propriétés des congruences entre entiers (développées précisément par GAUSS) au lieu des propriétés de divisibilité. Un calcul classique montre que, si l'entier b n'a aucun facteur carré, il est nécessaire, pour que l'équation (1) ait des solutions en entiers x, y, z non tous nuls, que la congruence:

$$x^2 - ay^2 \equiv 0, \pmod{b}, \tag{3}$$

admette des solutions en entiers x, y telles que y soit premier avec b. Ces dernières solutions peuvent d'ailleurs se déduire des solutions c_i, si elles existent, de la congruence:

$$t^2 - a \equiv 0, \pmod{b} \tag{4}$$

au moyen des formules:

$$x = c_i\lambda_1 + b\lambda_2, \qquad y = \lambda_1.$$

On reconnaît que l'ensemble des nombres algébriques:

$$x+\theta y = (\theta+c_i)\lambda_1+m\lambda_2 \qquad (\theta^2—a)$$

forme un idéal canonique, de norme a, de racine c_i, du corps quadratique engendré par $\theta = \sqrt{a}$, si toutefois a n'est pas congru à $+1$, (mod. 4) (définition constructive des idéaux canoniques (**7**, **1**)).

Limitons-nous provisoirement aux entiers a, sans facteurs carrés, et non congrus à $+1$, (mod. 4). Il est classique de comparer les solutions d'une congruence suivant un entier composé aux solutions de la même congruence suivant les facteurs de cet entier. Cette comparaison, faite pour la congruence (3), conduit aux règles de multiplication des idéaux canoniques (**15**) et à la décomposition de ses idéaux en produits d'idéaux correspondant aux seuls modules premiers (**15**, **3**).

Si on essaie d'appliquer la même méthode aux entiers a, sans facteurs carrés, congrus à $+1$, (mod. 4), on découvre une anomalie. Les deux congruences:

$$t^2—a \equiv 0, \ (\text{mod.}2),$$
$$t^2—a \equiv 0, \ (\text{mod. } 4),$$

ont les mêmes solutions (les entiers t impairs); la congruence:

$$t^2—a \equiv 0, \ (\text{mod. } 8),$$

a ou n'a pas de solutions suivant que a est congru à $+1$ ou à 3, (mod. 8). Les solutions des congruences (3) suivant les modules impairs conduisent encore aux mêmes règles de multiplication et de décomposition des idéaux canoniques que dans le cas précédent. Mais l'étude de cette congruence suivant les modules pairs ne conduit aux mêmes règles que si on fait jouer au module 8 le rôle joué précédemment par le module premier 2.

Mais, si on remplace les congruences (3) et (4) par les congruences:

$$x^2+xy—Ny^2 \equiv 0, \ (\text{mod. } b),$$
$$t^2+t—N \equiv 0, \ (\text{mod. } b),$$

avec $N = (1—a):4$, l'anomalie précédente disparaît; les règles

de multiplication et de décomposition des idéaux canoniques sont les mêmes pour tous les modules composés.

Ce changement de congruences revient encore à remplacer les nombres $\alpha = x+ay$, x, y entiers, par les nombres $\alpha = x+\theta y$, x, y entiers, où θ est une des racines de l'équation:

$$x^2+x-N = 0.$$

Ces derniers nombres sont bien les entiers du corps considéré.

On découvre une anomalie analogue en essayant d'appliquer la méthode à un entier a possédant des facteurs carrés. Si p est un nombre premier dont le carré divise a, les deux congruences

$$t^2-a \equiv 0, \ (\text{mod. } p),$$
$$t^2-a \equiv 0, \ (\text{mod. } p^2),$$

ont les mêmes solutions (les entiers divisibles par p); la congruence:

$$t^2-a \equiv 0, \ (\text{mod. } p^2),$$

peut n'admettre aucune solution. On peut encore faire disparaître l'anomalie en supprimant les facteurs carrés de a.

On est ainsi conduit à la construction utilisée du corps quadratique, et à la définition classique des entiers du corps.

F. C.

ERRATA

Au chapitre I, paragraphe 2 (tome VI, fascicule 2), page 87:

ligne 9 en commençant par le bas:
lire $r^2+Srs+Ns^2$ au lieu de $r^2-Srs+Ns^2$;

ligne 7 en commençant par le bas:
lire $(r^2+Srs+Ns^2)$ au lieu de $(r^2-Ss+Ns^2)$.