

MARIE-FRANCE GUÉHO

**Nombre de classes d'idéaux d'une algèbre de quaternions
totalement définie sur $\mathbb{Q}$**

Séminaire de théorie des nombres de Bordeaux (1969-1970), exp. n° 11, p. 1-7

http://www.numdam.org/item?id=STNB_1969-1970____A11_0

© Université Bordeaux 1, 1969-1970, tous droits réservés.

L'accès aux archives du séminaire de théorie des nombres de Bordeaux implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

NOMBRE DE CLASSES D'IDEAUX D'UNE ALGÈBRE DE
QUATERNIONS TOTALEMENT DÉFINIE SUR $\mathbb{Q}$

par

Marie-France GUÉHO

-:-:-

Cet exposé a pour but de donner des résultats montrés par Eichler dans : "Über die Klassenzahl total definiter quaternionen algebren".

Un exposé préliminaire a été fait au séminaire d'Arithmétique et d'Algèbre (exposé n° 16, année 1969-70) introduisant les notions et démontrant les théorèmes utilisés et non démontrés dans l'étude qui suit. On pourra également se reporter à "Algebren" de Deuring.

I. - RAMIFICATION DANS UNE ALGÈBRE DE QUATERNIONS

Soit k un corps de nombres, H une algèbre de quaternions sur k . Un premier p de k est ramifié si $H \otimes k_p$ est un corps gauche.

On appelle idéal de base de H le produit des premiers ramifiés finis. On le notera d .

Si Δ est le discriminant de H , on a la propriété $\Delta = d^2$. Donc un premier fini est ramifié si et seulement si il divise le discriminant.

Une algèbre de quaternions est caractérisée par son idéal de base et sa ramification à l'infini, car si p est ramifié $H \otimes k_p$ est le corps gauche de rang 4 sur k_p , si non, $H \otimes k_p$ est isomorphe à $M_2(k_p)$. Hasse a montré que 2 algèbres de quaternions sont isomorphes si et seulement si toutes leurs localisées le sont.

On sait également que le nombre de premiers ramifiés est pair.

II. - FORMULE D'EICHLER

Une algèbre de quaternions H sur un corps de nombres k est totalement définie si k est totalement réel et si $\text{Nrd}(x)$ est totalement positive pour tout x de H .

Soient H une algèbre de quaternions totalement définie sur un corps de nombres k .

Soient h_k le nombre de classes de k ,
 ζ_k la fonction zêta de k ,
 Δ_k le discriminant de k ,
 d l'idéal de base de H ,
 h le nombre de classe de H ,
 $\mathcal{O}_i$ un ordre maximal de H ,
 $W_{\mathcal{O}_i}$ l'indice fini du groupe des unités de k dans celui de $\mathcal{O}_i$.

Eichler a montré la formule suivante :

$$\frac{2h_k \zeta_k(2) |\Delta_k|^{3/2}}{(2\pi)^{2[k:\mathbb{Q}]}} \prod_{p|d} [N_{k/\mathbb{Q}}(p) - 1] = \sum_{i=1}^h \frac{1}{W_{\mathcal{O}_i}}.$$

$\mathcal{O}_i$ parcourant l'ensemble des ordres à droites d'un système de représentants des classes à gauche d'idéaux à gauche pour un ordre donné.

En utilisant l'équation fonctionnelle de la fonction zêta, on peut écrire cette formule d'une façon différente :

$$\frac{(-1)^{[k:\mathbb{Q}]} h_k \zeta_k(-1)}{2^{[k:\mathbb{Q}] - 1}} \prod_{p|d} [N_{k/\mathbb{Q}}(p) - 1] = \sum_{i=1}^h \frac{1}{W_{\mathcal{O}_i}}.$$

III. - SOUS GROUPES QUATERNIONIQUES FINIS SUR $\mathbb{R}$

H étant le corps de quaternions usuel sur $\mathbb{R}$, Coxeter a trouvé tous les sous-groupes finis de H^* . Ce sont

- Les groupes cycliques.
- Les groupes quaternioniques généralisés d'ordre $4n$ de générateurs σ, τ tels que :

$$\sigma^{2n} = 1, \quad \sigma^n = \tau^2, \quad \tau \sigma \tau^{-1} = \sigma^{-1}.$$

- Trois groupes particuliers

E_{24} engendrés par σ, τ tels que $\sigma^3 = \tau^3 = (\sigma\tau)^2, \sigma^6 = 1,$

E_{48} avec les relations $\sigma^3 = \tau^4 = (\sigma\tau)^2, \sigma^6 = 1,$

E_{120} avec les relations $\sigma^3 = \tau^5 = (\sigma\tau)^2, \sigma^6 = 1.$

IV. - NOMBRE DE CLASSES D'UNE ALGÈBRE DE QUATERNIONS TOTALEMENT DÉFINIE SUR $\mathbb{Q}$

THEOREME. Soit H une algèbre de quaternions totalement définie sur $\mathbb{Q}$
d'idéal de base (d) , de nombre de classes h .

Si $d = 2$ ou si $d = 3$, $h = 1$. Sinon

$$h = \frac{\varphi(d)}{12} + \frac{1}{2} h_2 + \frac{2}{3} h_3,$$

où

$\left\{ \begin{array}{l} h_2 = 2^{u-1} \\ h_2 = 0 \end{array} \right.$	<u>si u est le nombre de diviseurs premiers</u> <u>impairs de d, lorsque aucun d'entre eux</u> <u>n'est congru à 1 modulo 4,</u>
	<u>sinon</u>
$\left\{ \begin{array}{l} h_3 = 2^{v-1} \\ h_3 = 0 \end{array} \right.$	<u>si v est le nombre de diviseurs premiers</u> <u>de d différents de 3, lorsque aucun</u> <u>d'entre eux n'est congru à 1 modulo 3,</u>
	<u>sinon.</u>

Démonstration. La preuve de ce théorème est assez longue, on la divisera en plusieurs parties.

(1) La formule d'Eichler dans ce cas particulier s'écrit

$$\frac{\varphi(d)}{12} = \sum_{i=1}^h \frac{1}{W_{\mathcal{O}_i}} .$$

(2) Estimons les $W_{\mathcal{O}_i}$. -1 et $+1$ étant les unités de $\mathcal{Q}$, $W_{\mathcal{O}_i} = \frac{1}{2} \times$ ordre du groupe des unités de $\mathcal{O}_i$.

Une unité de $\mathcal{O}_i$ engendre une extension sur $\mathcal{Q}$ de degré au plus 2 , puisque H n'est pas commutative, donc est d'ordre 1 , 2 , 3 , 4 ou 6 .

Les groupes quaternioniques finis n'admettant pas d'unité d'ordre différent sont: E_{24} ; les groupes quaternioniques généralisés d'ordre 4 , 8 , 12 ; les groupes cycliques d'ordre 4 , 6 (l'ordre doit être pair).

Donc $W_{\mathcal{O}_i} = 1 , 2 , 3 , 4 , 6$ ou 12.

(3) Eliminons les cas spéciaux :

a - Remarquons que le groupe quaternionique généralisé d'ordre 8 est contenu dans E_{24} . Il est engendré par σ , τ tels que $\sigma^2 = \tau^2 = (\sigma\tau)^2$, $\sigma^4 = 1$. Donc $H = \mathcal{Q}_{[-1, -1]}$, ($\mathcal{Q}_{[-\alpha, -\beta]}$ désignant l'algèbre de base 1, i, j, ij telle que $i^2 = -\alpha$, $j^2 = -\beta$, $ij = -ji$) , l'idéal de base de $\mathcal{Q}_{[-1, -1]}$ est (2) . On dit que 2 est le nombre de base. On ne peut avoir $W_{\mathcal{O}_i} = 12$ que si $d = 2$.

$$\text{Or si } d = 2 , \quad \frac{\varphi(d)}{12} = \frac{1}{12} .$$

Donc $h = 1$.

Remarquons que l'ordre engendré par $(1, i, j, \frac{1+i+j+ij}{2})$ ayant 4 pour discriminant est maximal.

Son groupe d'unités est E_{24} .

b - Si H contient le groupe quaternionique généralisé d'ordre 12 engendré par $\sigma^3 = \tau^2 = (\sigma\tau)^2 = -1$. En posant $i = \tau$, $j = 2\sigma - 1$, on vérifie que

$$i^2 = -1 , \quad j^2 = -3 , \quad ij = -ji ,$$

$$\text{donc } H = \mathcal{Q}_{[-1, -3]} \quad \text{et} \quad d = 3 , \quad \frac{\varphi(3)}{12} = \frac{1}{6} .$$

Donc $h = 1$. Tous les ordres maximaux ont pour groupe d'unités, le groupe quaternionique généralisé d'ordre 12 .

(4) On a donc montré, si $d = 2$ ou $d = 3$, alors $h = 1$. Sinon

$$h = \frac{\varphi(d)}{12} + \frac{1}{2} h_2 + \frac{2}{3} h_3 \quad ; \quad h_2, h_3 \in \mathbb{N}.$$

En effet, on a montré

$$\frac{\varphi(d)}{12} = h_1 + \frac{h_2}{2} + \frac{h_3}{3} \quad ; \quad h_1, h_2, h_3 \in \mathbb{N}.$$

Or $h = h_1 + h_2 + h_3$. D'où en éliminant h_1

$$h = \frac{\varphi(d)}{12} + \frac{h_2}{2} + \frac{2}{3} h_3.$$

(5) Calcul de h_2 . h_2 est le nombre de classes des idéaux à gauche d'un ordre donné, dont l'ordre à droite a un groupe d'unités cyclique d'ordre 4.

Pour que h_2 soit non nul, il faut donc que H contienne une unité d'ordre 4, donc qu'aucun diviseur de d ne soit congru à 1 modulo 4.

(La démonstration se trouve dans Korinek. Elle est élémentaire, mais un peu longue pour cet exposé).

Si 2 ordres maximaux $\mathcal{O}_1$ et $\mathcal{O}_2$ contiennent une unité d'ordre 4, i_1 et i_2 respectivement, tout automorphisme de H étant intérieur, $\exists \alpha \in H : i_2 = \alpha^{-1} i_1 \alpha$, donc $\alpha^{-1} \mathcal{O}_1 \alpha$ est un ordre du même type que $\mathcal{O}_1$ ayant même groupe d'unités que $\mathcal{O}_2$.

On en déduit que le nombre de types des ordres contenant une unité d'ordre 4 est égal au nombre de types des ordres contenant l'anneau des entiers de $\mathbb{Q}(\sqrt{-1})$. Cet anneau est principal, si deux ordres maximaux le contiennent, leur idéal de distance est principal, les deux ordres sont donc du même type.

Nous sommes conduits à chercher lorsque h_2 est différent de 0, le nombre d'idéaux ambiges principaux d'un ordre maximal contenant $i = \sqrt{-1}$.

Comme aucun diviseur de d n'est congru à 1 modulo 4, lorsque $h_2 \neq 0$, $\mathbb{Q}[-1, -d]$ a d comme nombre de base et est isomorphe à H , donc $\mathcal{O}$ contient ω tel que $\omega^2 = -d$.

$\mathcal{O}\omega$ est un idéal ambige principal (ambige = entier bilatère diviseur de la différente).

Lorsque d est pair, $\mathcal{O}(1+i)$ est ambige principal. Soit $\mathcal{O}\alpha$ un idéal entier bilatère, $\alpha^{-1}i\alpha$ est une unité de $\mathcal{O}$ d'ordre 4, donc $\alpha^{-1}i\alpha = \mp i$.

Deux cas se présentent : α ou $\omega\alpha$ commutent avec i ou ce qui est équivalent : α ou $\omega\alpha$ appartiennent à $Z[i]$. $\mathcal{O}\alpha$ et $\mathcal{O}\omega\alpha$ étant bilatères $(\mathcal{O}\alpha)^2 = \mathcal{O}n(\alpha)$ et $(\mathcal{O}\omega\alpha)^2 = \mathcal{O}n(\omega\alpha)$ si $\alpha \in Z[i]$ on aura :

$$\alpha^2 = \mp n(\alpha) \quad \text{ou} \quad \alpha^2 = \mp i n(\alpha) ,$$

d'où $\mathcal{O}\alpha = \mathcal{O}r$ ou $\mathcal{O}\alpha = \mathcal{O}(1+i)r$, $r \in \mathcal{O}$,

si $\omega\alpha \in Z[i]$, $\mathcal{O}\alpha = \mathcal{O}\omega r$ ou $\mathcal{O}\alpha = \mathcal{O}\omega(1+i)^{-1}r$.

On en déduit que les idéaux ambiges principaux sont $\mathcal{O}$, $\mathcal{O}\omega$, $\mathcal{O}(1+i)$, $\mathcal{O}\omega(1+i)^{-1}$ au plus.

On en déduit que nous aurons 2^{u-1} idéaux ambiges non équivalents si u désigne le nombre de diviseurs premiers impairs de d .

(6) Calcul de h_3 . Des considérations analogues non conduisent.

$\mathcal{O}(\sqrt{-3})$ étant principal, les ordres maximaux contenant une suite unité d'ordre 3 appartiendront au même type. Il en existe si $H \supset \mathcal{O}(\sqrt{-3})$, pour cela aucun diviseur premier de d ne doit être congru à 1 modulo 3. Dans ce cas, H est isomorphe à $\mathcal{O}(-3, -|d|)$, si $\omega^2 = -d$, $\rho^3 = 1$, si $\mathcal{O}$ est un ordre maximal contenant ρ , alors $\mathcal{O}$, $\mathcal{O}\omega$ sont les seuls idéaux ambiges principaux si d n'est pas divisible par 3, sinon on a $\mathcal{O}$, $\mathcal{O}\omega$, $\mathcal{O}(1+2\rho)$, $\mathcal{O}(1+2\rho)^{-1}\omega$.

On en déduit que nous aurons 2^{v-1} idéaux ambiges non équivalents si v désigne le nombre de diviseurs premiers différents de 3 de d .

V. - ALGÈBRE DE QUATERNIONS, TOTALEMENT DÉFINIES SUR $\mathcal{O}$ PRINCIPALES

Le théorème précédent permet de calculer rapidement les algèbres de quaternions totalement définies sur $\mathcal{O}$ qui sont principales.

d est un produit de premiers, d'exposant 1, en nombre impair,
donc $d > 13$ entraîne $\varphi(d) > 12$, donc $h > 1$ d'après la formule d'Eichler.

Si $d \leq 13$,

$$d = 13 \quad \frac{\varphi(d)}{12} = 1, \quad h_2 = h_3 = 0, \quad \text{donc } h = 1,$$

$$d = 11 \quad \frac{\varphi(d)}{12} = \frac{5}{6}, \quad h_2 = 1, \quad h_3 = 1, \quad \text{donc } h = 2,$$

$$d = 7 \quad \frac{\varphi(d)}{12} = \frac{1}{2}, \quad h_2 = 1, \quad h_3 = 0, \quad \text{donc } h = 1,$$

$$d = 5 \quad \frac{\varphi(d)}{12} = \frac{1}{3}, \quad h_2 = 0, \quad h_3 = 1, \quad \text{donc } h = 1,$$

$$d = 3 \quad h = 1,$$

$$d = 2 \quad h = 1.$$

Nous avons donc exactement cinq algèbres de quaternions totalement définies sur $\mathbb{Q}$, principales. Elles ont pour nombre de base : 2, 3, 5, 7, 13. (1)

(1) Remarque. On montre que, quel que soit d , il existe une et une seule algèbre de quaternions totalement définie de nombre de base d .

-:-:-:-