Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Marie-France Guého

Quaternions et $\zeta_k(-1)$

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 13, n° 2 (1971-1972), exp. n° 14, p. 1-7

<http://www.numdam.org/item?id=SDPP_1971-1972__13_2_A2_0>

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1971-1972, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » 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/

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
13e année, 1971/72, n° 14, 7 p.

14 février 1972

QUATERNIONS ET $\zeta_k(-1)$

par Marie-France GUÉHO

En 1937, EICHLER donne une formule reliant le nombre h de classes d'idéaux d'un corps de quaternions totalement défini sur un corps de nombres k et la valeur $\zeta_k(-1)$ au point -1 de la fonction zêta du corps k. Nous allons donner une forme nouvelle à ces résultats et en déduire des propriétés de h et de $\zeta_k(-1)$.

1. Groupe de Brauer.

Définitions.

- Une algèbre H de dimension finie sur un corps k est appelée une algèbre centrale simple sur k s'il existe un corps gauche D, de centre k, tel que H soit k-isomorphe à une algèbre de matrices sur D.

- Deux algèbres centrales simples sur k sont dites équivalentes si les corps gauches qui leur sont associés sont k-isomorphes.

- Le produit tensoriel munit par passage au quotient l'ensemble des classes d'une structure de groupe abélien ; ce groupe est le groupe de Brauer de k. On le note $Br(k)$.

Exemples.

- Si k est un corps fini ou algébriquement clos, $Br(k) = 0$.

- $Br(R) = Z/2Z$.

- Si k est un corps complet pour une valuation discrète à corps résiduel fini, on montre que :

$Br(k) = Q/Z$;

L'image dans $Br(k)$ d'un corps gauche de centre k, de dimension n^2 sur k, est de la forme a/n, avec $(a , n) = 1$;

Si L est une extension de k de degré ℓ, l'application de $Br(k)$ dans $Br(L)$, obtenue par extension des scalaires de k à L, est $\alpha \longrightarrow \ell\alpha$.

Groupe de Brauer d'un corps de nombres. - Si k est un corps de nombres, pour toute place v de k, notons k_v le complété de k pour la topologie définie par v. On montre que $Br(k)$ s'injecte naturellement dans $\bigoplus_v Br(k_v)$ et que la suite ci-dessous est exacte :

$$0 \longrightarrow Br(k) \longrightarrow \bigoplus_v Br(k_v) \xrightarrow{\sigma} Q/Z \longrightarrow 0 ,$$

où σ est l'application définie par $\sigma((\alpha_v)) = \sum_v \alpha_v$.

Soit H une algèbre centrale simple sur k. Une place v de k est dite ramifiée dans H si l'image α_v de $H \otimes_k k_v$ dans $Br(k_v)$ n'est pas nulle. Si H est de dimension 4 sur k, alors $\alpha_v = 0$ ou $1/2$, et l'exactitude de la suite montre que le nombre de places ramifiées est pair. Lorsque k est totalement réel et que toute place réelle de k est ramifiée dans H, on dit que H est un corps de quaternions totalement défini sur k, et H est caractérisé par l'ensemble des places finies de k qui se ramifient.

2. Ordres maximaux et idéaux. Norme réduite.

Soient k un corps de nombres, d'anneau d'entiers A, et H une algèbre centrale simple sur k, de dimension n^2 sur k.

Ordres et idéaux.

Un réseau de A dans H est appelé un ordre de H s'il contient 1 et si c'est un anneau d'entiers. Tout ordre est contenu dans un ordre maximal ; les ordres considérés dans la suite seront toujours des ordres maximaux.

Soit O un ordre ; un O-module à gauche P, projectif, de type fini, est appelé un idéal à gauche de O. Soit $P^{-1} = \{x \in H \mid Px \in O\}$, alors $O' = P^{-1} P$ est un ordre maximal, l'idéal P (resp. P^{-1}) à gauche de O (resp. O') est à droite de O' (resp. O). Si $P \subset O$, on dit que P est un idéal entier.

Deux idéaux P et P' sont dits équivalents s'il existe $x \in H$ tel que $P' = Px$. Leurs ordres à droite vérifient $P'^{-1} P' = x^{-1} P^{-1} Px$. Deux ordres O et O' tels que $O' = x^{-1} Ox$ sont dits du même type. Le nombre h des classes des idéaux à gauche d'un ordre est fini, indépendant du choix de l'ordre et appelé le nombre de classes d'idéaux de H.

Norme réduite. - Soit K un corps algébriquement clos contenant k, on sait que $H \otimes_k K$ est K-isomorphe à $M_n(K)$. On note i l'injection naturelle de H dans $H \otimes_k K$, et λ un K-isomorphisme de $H \otimes_k K$ sur $M_n(K)$. Si $x \in H$, le déterminant de $\lambda \cdot i(x)$ est indépendant du choix de λ, K, appartient à k, et est appelé la norme réduite de x. On le note $Nrd(x)$. Si P est un idéal à gauche de O, pour toute place finie v de k, on note P_v (resp. O_v) l'image de P (resp. de O) dans $H \otimes_k k_v$. On sait qu'il existe $b_v \in H \otimes_k k_v$ tel que $P_v = O_v b_v$. Par définition, la norme réduite de P est

$$Nrd(P) = \prod_v (Nrd(b_v)) .$$

3. Formule d'Eichler.

Nous supposons dans la suite que H désigne un corps de quaternions totalement défini sur un corps de nombres k. La relation d'équivalence considérée dans le groupe des idéaux de k est l'équivalence au sens restreint.

La fonction zêta de H relative à une classe R d'idéaux à gauche d'un ordre O

est définie par

$$\zeta_H(s\ ,\ R) = \Sigma_P\ [N_{k/Q} \circ \mathrm{Nrd}(P)]^{-2s}\ ,$$

où $N_{k/Q}$ est la norme absolue de k, et où P parcourt l'ensemble des idéaux entiers de la classe R. La fonction zêta de H est

$$\zeta_H(s) = \Sigma_R\ \zeta_H(s\ ,\ R)\ .$$

Ces fonctions sont méromorphes dans C, et ont pour résidu au point 1 :

$$\lim_{s=1}(s - 1)\ \zeta_H(s\ ,\ R) = \lambda/w_R\ ,$$

$$\lim_{s=1}(s - 1)\ \zeta_H(s) = \lambda/2^{n-1}\ h_k\ \zeta_k(-1)\ \Pi_{y\,|\,\Delta_H}\ (1 - N_{k/Q}(y))\ ,$$

où :

w_R est l'indice dans le groupe des unités de l'ordre à droite d'un idéal de classe R, du sous-groupe formé par les unités de k,

λ est une constante ne dépendant que du corps k,

h_k, $\zeta_k(\cdot)$, n désignent respectivement le nombre de classes d'idéaux (au sens ordinaire), la fonction zêta, le degré absolu du corps k,

Δ_H est le produit des idéaux premiers de k correspondant aux places finies ramifiées dans H.

On pose :

$$\zeta_k^{(H)}(-1) = \zeta_k(-1)\Pi_{y\,|\,\Delta_H}(1 - N_{k/Q}(y))\ ,$$

et on obtient la formule d'Eichler en écrivant l'égalité entre résidus

$$\lim_{s=1}(s - 1)\ \zeta_H(s) = \Sigma_R\ \lim_{s=1}(s - 1)\ \zeta_H(s\ ,\ R)\ .$$

FORMULE D'EICHLER. - Avec les notations précédentes,

$$\zeta_k^{(H)}(-1) = 2^{n-1}/h_k\ \Sigma_R\ 1/w_R\ .$$

La norme réduite définissant un homorphisme surjectif de H^* (H privé de 0) sur le groupe des éléments de k totalement positifs, les idéaux de classe R ont leurs normes réduites équivalentes dans k (au sens restreint). On peut écrire :

$$\Sigma_R\ 1/w_R = \Sigma_X\ \Sigma_{\mathrm{Nrd}(R)\subset X}\ 1/w_R\ ,$$

avec X parcourant l'ensemble des classes d'idéaux de k.

Nous allons montrer que $\Sigma_{\mathrm{Nrd}(R)\subset X}\ 1/w_R$ est indépendant du choix de X.

Soit P', un idéal à gauche de 0, de norme réduite dans X^{-1}, d'ordre à droite $0'$. L'application $Q \longrightarrow P'Q$ définit par passage au quotient une bijection de l'ensemble des classes des idéaux à gauche de $0'$, de norme réduite dans X, sur l'ensemble des classes des idéaux à gauche de 0, de norme réduite principale. Mais $\Sigma_{\mathrm{Nrd}(R)\subset X}\ \zeta_H(s\ ,\ R)$ est indépendant du choix de l'ordre 0, il en est de même pour son résidu au point $s = 1$. La bijection précédente montre que ce résidu est aussi indépendant du choix de la classe X. On obtient

$$\zeta_k^{(H)}(-1) = 2^{n-1}\, h_k^+/h_k \sum_{\mathrm{Nrd}(R)\subset X} 1/w_R ,$$

où h_k^+ est le nombre de classes d'idéaux de k (au sens restreint).

Nous remarquons que w_R ne dépend que du type T des ordres à droite des idéaux de classe R, aussi nous le notons w_T, et en appelant $\mathfrak{C}_X$ l'ensemble des types des ordres à droite des idéaux de norme réduite dans X, l'égalité précédente s'écrit

$$\zeta_k^{(H)}(-1) = 2^{n-1}\, h_k^+/h_k \sum_{T\in\mathfrak{C}_X} n_T/w_T ,$$

où n_T est le nombre de classes des idéaux de norme réduite dans X, dont l'ordre à droite est du type T. L'application $X \longrightarrow \mathfrak{C}_X$ définit sur l'ensemble des types d'ordres de H, une partition telle que deux types d'ordres T et T' sont équivalents (c'est-à-dire, appartiennent à un même $\mathfrak{C}_X$) si et seulement s'il existe un idéal P de norme réduite principale, à gauche d'un ordre du type T, à droite d'un ordre du type T'. Donc n_T ne dépend que de la classe du type T.

Considérons maintenant un idéal P, de norme réduite dans X, dont l'ordre à droite O' est du type T ; l'application $Q \longrightarrow PQ$ définit par passage au quotient une bijection des classes des idéaux de norme réduite principale, bilatères de O', sur les classes des idéaux de norme réduite dans X, dont l'ordre à droite est du type T.

Nous montrons ensuite que n_T est une puissance de 2. Les normes réduites caractérisent les idéaux bilatères d'un ordre O et se mettent de façon unique sous la forme QB^2, où B est un idéal de k et Q un idéal entier de k divisant Δ_H. Soient (A_i), $i = 1, \dots, 2^e$, un système de représentants des classes d'idéaux de k, de carré principal, et $(\mathfrak{P}_j)$, $j = 1, \dots, 2^{s'}$, des idéaux bilatères de O, de norme réduite $Q_j B_j^2$ principale, où (Q_j), $j = 1, \dots 2^{s'}$, est l'ensemble des diviseurs de Δ_H de classe un carré. Les idéaux bilatères de O, de norme réduite principale, s'écrivent de façon unique $\mathfrak{P}_j A_j x$, $x \in H$, et leur nombre de classes n_T divise $2^{e+s'}$. On le note 2^t.

Enfin, soient E_T le groupe des unités d'un ordre du type T, $\hat{w}_T$ l'ordre du sous-groupe de E_T formé des unités de norme réduite 1, E_k^+ le groupe des unités totalement positives de k. Nous avons les égalités suivantes :

$$2w_T = \hat{w}_T\, [\mathrm{Nrd}(E_T) : E_k^2] = 2^n\, \hat{w}_T\, [E_k^* : \mathrm{Nrd}(E_T)]^{-1} ,$$

$$h_k^+ = h_k\, 2^n\, [E_k : E_k^+]^{-1} ,$$

$$h_k^+/(2h_k\, w_T) = [E_k^+ : \mathrm{Nrd}(E_T)]/\hat{w}_T .$$

Nous avons montré le théorème suivant.

THÉORÈME. - Avec les notations précédentes,

$$\zeta_k^{(H)}(-1) = 2^{n+t} \sum_{T\in\mathfrak{C}} [E_k^+ : \mathrm{Nrd}(E_T)]/\hat{w}_T .$$

4. Classes d'idéaux.

Deux idéaux P et P' à gauche d'un ordre O,

1° appartiennent à la même classe, si, et seulement si, $P' = Px$, $x \in H$;

2° ont leurs ordres à droite du même type, si, et seulement si, $P' = QPx$, $x \in H$, Q idéal bilatère de O ;

3° ont les types de leurs ordres à droite équivalents, si, et seulement si, $P' = QPR$, Q idéal bilatère de O, $\mathrm{Nrd}(R)$ principale. Pour cela, il faut et il suffit que l'idéal $\mathrm{Nrd}(P)\,\mathrm{Nrd}(P')^{-1}$ soit équivalent dans k à la norme réduite d'un idéal bilatère.

On définit ainsi 3 relations d'équivalence dont les nombres de classes $h_1 = h$, h_2 (le nombre de types d'ordres), h_3 ne dépendent pas du choix de O. La norme réduite définit par passage au quotient, une application surjective des classes d'idéaux de H (au sens du (1°)) sur les classes d'idéaux de k et le nombre de classes des normes réduites des idéaux bilatères d'un ordre est $2^{s-s'-e}\, h_k^+$. On en déduit

$$h_3 = 2^{s'+e-s}.$$

Il est clair que l'on peut écrire

$$h_2 = \sum_{\mathcal{C}} n_{\mathcal{C}},$$

la somme étant effectuée sur les classes $\mathcal{C}$, au sens du (3°) et $n_{\mathcal{C}}$ désignant le nombre de types d'ordres de classe $\mathcal{C}$. Enfin nous avons

$$h = h_1 = \sum_R 1 = \sum_X \sum_{\mathrm{Nrd}(R)\subset X} 1 = \sum_X \sum_{\mathcal{C}_X} 2^t\, n_{\mathcal{C}} = h_k^+\, 2^{s-s'-e} \sum_{\mathcal{C}} 2^t\, n_{\mathcal{C}}.$$

THÉORÈME. - Avec les notations précédentes,

$$h = h_k^+\, 2^{s-s'-e} \sum_{\mathcal{C}} 2^t\, n_{\mathcal{C}}.$$

5. Application au nombre de classe d'idéaux d'un corps de quaternions.

PROPOSITION. - Il n'y a qu'un nombre fini de corps de quaternions totalement définis sur un corps de nombres de degré donné, ayant un nombre de classes donné.

En effet, h étant donné, $n_{\mathcal{C}}$ et 2^t ne peuvent prendre qu'un nombre fini de valeurs ; n étant donné, il en est de même pour w_n, donc aussi pour $\zeta_k(-1)$ et pour $\prod_{y \mid \Delta_H} (1 - N_{k/\mathbb{Q}}(y))$. Comme

$$\zeta_k(-1) = d_k^{3/2}\, \zeta_k(2)\, (2\pi)^{-2n}, \quad |\zeta_k(2)| > 1,$$

le discriminant de k ne peut prendre qu'un nombre fini de valeurs, d'où un nombre fini de possibilités pour k et Δ_H.

Remarque. - Il existe 13 algèbres de quaternions totalement définies sur un corps quadratique réel qui sont principales. Ce sont les algèbres H, avec Δ_H égal à

1 , $\mathfrak{P}_2$, $5\mathfrak{P}_2$, $\mathfrak{p}_2\mathfrak{p}_7^{(1)}$, $\mathfrak{p}_2\mathfrak{p}^{(2)}$, sur $Q(\sqrt{2})$,

1 , $2\mathfrak{p}_5$, $2\mathfrak{p}_{11}^{(1)}$, $2\mathfrak{p}_{11}^{(2)}$, sur $Q(\sqrt{5})$,

1 , $2\mathfrak{p}_3^{(1)}$, $2\mathfrak{p}_3^{(2)}$, sur $Q(\sqrt{13})$,

1 sur $Q(\sqrt{17})$.

Dans cet énoncé, $\mathfrak{p}_2$, $\mathfrak{p}_7^{(1)}$, $\mathfrak{p}_7^{(2)}$, $\mathfrak{p}_5$, $\mathfrak{p}_{11}^{(1)}$, $\mathfrak{p}_{11}^{(2)}$, $\mathfrak{p}_3^{(1)}$, $\mathfrak{p}_3^{(2)}$ désignent les idéaux premiers du centre de l'algèbre au-dessus du nombre premier écrit en indice.

6. Application à $\zeta_k(-1)$.

1° Pour tout nombre premier p et pour tout entier m , soit $x_{p,m}$ une racine d'ordre p^m de l'unité, et soit $n_k(p)$ le plus grand des entiers m tels que $[k(x_{p,m}) : k] \leqslant 2$. Le p. p. c. m. des ordres des groupes finis de quaternions sur k est [4]

$$w = 2\prod_p p^{n_k(p)} ,$$

on a donc

$$w\zeta_k^{(H)}(-1) \in 2^n Z .$$

On en déduit un résultat démontré par J.-P. SERRE [5].

PROPOSITION. - Avec les notations précédentes, $w\zeta_k(-1) \in 2^n Z$.

C'est immédiat, si n est pair, car il existe H tel que $\Delta_H = (1)$. Si n est impair, il suffit de considérer les corps de quaternions totalement définis sur k tels que $\Delta_H = (\mathfrak{p}_2)$ et $\Delta_H = (\mathfrak{p}_q)$, où q parcourt l'ensemble des nombres premiers divisant $1 - N_{k/Q}(\mathfrak{p}_2)$, en notant $\mathfrak{p}_2$ (resp. $\mathfrak{p}_q$) un idéal premier de k au-dessus de 2 (resp. q).

2° Soit $e_k(2)$ l'exposant de 2 dans $\zeta_k(-1)$. On a $e_k(2) = n - n_k(2) - 1$, si h_k^+ est impair, et si $(2) = \mathfrak{p}_2^{2^{n_k(2)-2}}$ est la décomposition de l'idéal (2) dans k.

Soit H tel que $\Delta_H = (1)$ (resp. $\Delta_H = \mathfrak{p}_2$) si n est pair (resp. n impair), H est le corps usuel de quaternions sur k de base 1 , i , j , ij , avec $i^2 = j^2 = -1$, $ij = -ji$. Comme h_k^+ est impair, $e = 0$, $s' = s$, $h_3 = 0$, $t \leqslant s$. Si n est pair, $s = 0$; si n est impair, $s = 1$, mais $t = 0$ (En effet, soit O un ordre de H contenant $x_{2,n_k(2)} \in k(i)$, et j , l'idéal premier, bilatère de O , au-dessus de 2 , est engendré par l'idéal premier P_2 , au-dessus de 2 dans $k(i)$ [4], qui est principal). On a donc

$$\zeta_k^{(H)}(-1) = 2^n \Sigma_T 1/\hat{w}_T .$$

Tout ordre de type T , tel que $\hat{w}_T = 2^{n_k(2)+1}$, s'envoie par un automorphisme intérieur de H sur un ordre contenant $x_{2,n_k(2)}$ et j . Cet ordre est unique si

n est impair ; si n est pair, il y en a 2 qui sont du même type : 0 et $P_2^{-1} 0 P_2$. L'unicité du type d'ordre tel que $\hat{w}_T = 2^{n_k(2)+1}$ montre que $e_k(2) = n - n_k(2) - 1$.

Exemple. - Si k_m est le sous-corps réel maximal de $Q(x_{2,m})$, l'exposant de 2 dans $\zeta_{k_m}(-1)$ est

$$e_{k_m}(2) = 2^{m-2} - m - 1 .$$

On montre même, à l'aide des nombres de Bernoulli généralisés, que le quotient $\zeta_{k_{m+1}}(-1)/\zeta_{k_m}(-1)$ est un entier, et que $\zeta_{k_m}(-1) \in 2^{2^{m-2}-m-1} Z$, pour $m \geqslant 5$.

3° PROPOSITION. - On a

$$e_k(2) = -2 , \text{ pour } k = Q , Q(\sqrt{2}) ,$$

$$e_k(2) = -1 , \text{ pour } k = Q(\sqrt{2+\sqrt{2}}) , Q(\sqrt{m}) ,$$

avec m premier, $m \equiv -3 \bmod 8$, éventuellement pour les corps $Q(\sqrt{m})$ avec $m \equiv 2 \bmod 4$ ou $m \equiv 3 \bmod 8$

$$e_k(2) \geqslant 0 \text{ dans les autres cas.}$$

Les cas $k = Q(\sqrt{2})$, $Q(\sqrt{2+\sqrt{2}})$, Q sont des cas particuliers de l'exemple précédent. Il reste à étudier les corps quadratiques $Q(\sqrt{m})$, où m est un entier sans facteurs carrés, différent de 2 . Le cas m premier, $m \equiv -3 \bmod 8$, est un cas particulier de (2). Pour la démonstration du reste de la proposition, on pourra se reporter à [4].

BIBLIOGRAPHIE

[1] COXETER (H. S. M.). - The binary polyhedral groups and other generalizations of the quaternion group, Duke math. J., t. 7, 1940, p. 367-379.

[2] DEURING (Max). - Algebren. - Berlin, J. Springer, 1935 (Ergelnisse der Mathematik, 4, Heft 1).

[3] EICHLER (M.). - Über die Idealklassenzahl total definiter Quaternionenalgebren, Math. Z., t. 43, 1937, p. 102-109.

[4] GUEHO (Marie-France). - Corps de quaternions sur un corps de nombres algébriques, Thèse 3e cycle, Bordeaux, 1972.

[5] GUEHO (Marie-France). - Corps de quaternions et fonction zêta au point -1 , C. R. Acad. Sc. Paris, t. 274, 1972, Série A, p. 296-298.

[6] SERRE (J.-P.). - Cohomologie des groupes discrets, Prospects in Mathematics, p. 77-169. - Princeton, Princeton University Press, 1971 (Annals of Mathematics Studies, 70).

(Texte reçu le 5 juin 1972)

Marie-France GUEHO
Université de Bordeaux-I
U. E. R. de Mathématiques
351 cours de la Libération
33405 TALENCE