

Sommes de Gauss attachées aux caractères quadratiques: une conjecture de Pierre Conner.

Autor(en): **Kahn, Bruno**

Objektyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **62 (1987)**

PDF erstellt am: **11.09.2024**

Persistenter Link: <https://doi.org/10.5169/seals-47359>

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.

Sommes de Gauss attachées aux caractères quadratiques: une conjecture de Pierre Conner

BRUNO KAHN

Soit p un nombre premier et K une extension finie de \mathbb{Q}_p . Notons v la valuation discrète (normalisée) de K , O_K l'anneau de valuation de v , $U = O_K^*$ le groupe des unités de O_K et, pour $i > 0$, $U_i = \{x \in K \mid v(x - 1) \geq i\}$ ($U_0 = U$). Si χ est un homomorphisme continu de K^* dans $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$, c'est-à-dire un caractère de K^* , on appelle conducteur de χ l'entier $f(\chi) = \inf \{i \geq 0 \mid \chi(U_i) = \{1\}\}$. A un tel χ on associe un nombre complexe de module 1 [6, p. 94]:

$$W(\chi) = q^{-f/2} \sum_{x \in U/U_f} \chi(d^{-1}x)^{-1} \psi_K(d^{-1}x),$$

où q est le cardinal du corps résiduel de O_K , $f = f(\chi)$, d est un générateur de $\mathcal{M}^f \mathcal{D}_K$ (\mathcal{M} idéal maximal de O_K , \mathcal{D}_K différentielle de K/\mathbb{Q}_p) et ψ_K est le caractère additif de K défini par la composition

$$K \xrightarrow{\text{Tr}_{K/\mathbb{Q}_p}} \mathbb{Q}_p \rightarrow \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \mathbb{Q}/\mathbb{Z} \xrightarrow{e^{2\pi}} S^1.$$

Supposons χ quadratique, i.e. $\chi^2 = 1$. Alors χ est de la forme $x \mapsto (-1)^{(a,x)}$, où $(a, x) \in \mathbb{Z}/2$ est le symbole de Hilbert de deux éléments de K^* ; ainsi les caractères quadratiques sont en bijection avec les éléments de K^*/K^{*2} . Si $a \in K^*$, notons $\rho_a(x) = (-1)^{(a,x)}$; on a la formule, pour $a, b \in K^*$ [6, p. 126, cor. 2]:

$$W(\rho_a \rho_b) = W(\rho_a)W(\rho_b)(-1)^{(a,b)}. \tag{1}$$

En faisant $a = b$, on en déduit que $W(\rho_a)$ est une racine 4^e de l'unité. Soit $w(a) \in \frac{1}{4}\mathbb{Z}/\mathbb{Z}$ tel que $W(\rho_a) = i^{4w(a)}$; on a donc:

$$w(ab) = w(a) + w(b) + \frac{1}{2}(a, b).$$

La fonction w définit donc une fonction quadratique de K^*/K^{*2} dans $\frac{1}{4}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}_2/\mathbb{Z}_2$, relevant le symbole de Hilbert. Suivant une idée de Pierre

Conner, on peut considérer sa classe dans $WQ(\mathbb{Q}_2, \mathbb{Z}_2)$ [4, App] et lui associer une somme de Gauss "à la Weil" $\gamma(w)$ (cf par exemple [2, p. 26-17]). Par définition même, on a:

$$\overline{\gamma(w)} = (K^* : K^{*2})^{-1/2} \sum_{a \in K^*/K^{*2}} W(\rho_a).$$

Ainsi, le membre de droite de l'égalité ci-dessus est une *racine 8^{ème} de l'unité*. La conjecture de Conner, démontrée dans cet article, consiste à identifier $\gamma(w)$ à une somme de Gauss attachée à une autre forme quadratique. Pour l'énoncer, notons Q_K la forme quadratique sur \mathbb{Q}_p définie par $X \mapsto \text{Tr}_{K/\mathbb{Q}_p} x^2$ ($x \in K$); par le procédé de [2, §7], on lui associe une racine 8^{ème} de l'unité $\gamma(Q_K)$.

THEOREME 1. *On a $\gamma(w) = \gamma(Q_K)$.*

Je donnerai de ce théorème deux démonstrations: une démonstration locale et une démonstration globale. La démonstration globale est due à Pierre Conner, la démonstration locale est due à moi-même.

Afin de préparer les démonstrations, notons, pour tout $a \in K^*$, $Q_{K,a}$ la forme quadratique $x \mapsto \text{Tr}_{K/\mathbb{Q}_p} ax^2$ et $\gamma(a) = \gamma(Q_{K,a})$. D'après [2, prop. 8], on a:

$$W(\rho_a) = \gamma(a)\gamma(1)^{-1}; \tag{2}$$

la formule à démontrer se réduit donc à:

$$(K^* : K^{*2})^{-1/2} \sum_{a \in K^*/K^{*2}} \gamma(a) = 1.$$

Première démonstration. Posons $A = K^*/K^{*2}$. Soit $A_{nr} \subset A$ le sous-groupe formé des classes de carrés non-ramifiées (i.e. telles que $f(\rho_a) = 0$): c'est un groupe d'ordre 2. Posons $B = U/A_{nr}U^2$: c'est un sous-quotient de A , et on a $|B| = 2^n$, avec $n = 0$ si $p \neq 2$, $n = [K : \mathbb{Q}_2]$ si $p = 2$. De plus, $|A| = 4|B|$.

(Dans cet article, on convient de noter $|X|$ le cardinal d'un ensemble fini X .)

LEMME 1. *Soit δ un générateur de \mathcal{D}_K . Posons, pour $a \in K^*$, $\gamma'(a) = \gamma(\delta a)$. Alors, si $a \in U$, $\gamma'(a)$ ne dépend que de la classe de a dans B , et on a:*

$$\sum_{a \in A} \gamma(a) = \sum_{a \in A} \gamma'(a) = 2 \sum_{a \in B} \gamma'(a).$$

En effet, les formules (1) et (2) ci-dessus entraînent, pour $a, b \in A$:

$$\gamma(ab) = \gamma(a)\gamma(b)\gamma(1)^{-1}(-1)^{(a,b)}. \quad (3)$$

Soit $a \in A$, $u \in A_{nr}$. On déduit de (3):

$$\gamma'(au) = \gamma(\delta au) = \gamma(\delta a)\gamma(u)\gamma(1)^{-1}(-1)^{(\delta a,u)}.$$

Mais $W(\rho_u) = (-1)^{(\delta,u)}$: cela résulte de la définition de W . On en conclut (voir (2)) que:

$$\gamma'(au) = \gamma'(a)(-1)^{(a,u)} = \gamma'(a)(-1)^{v(a)} \text{ si } u \text{ est non-trivial.} \quad (4)$$

Si $a \in U$, on a donc $\gamma'(au) = \gamma'(a)$, ce qui prouve la première affirmation du lemme. Dans celui-ci, la première égalité est triviale; pour la deuxième, on écrit:

$$\sum_{a \in A} \gamma'(a) = \sum_{a \in U/U^2} \gamma'(a) + \sum_{a \notin U/U^2} \gamma'(a) = \sum_{a \in U/U^2} \gamma'(a) + \sum_{a \in U/U^2} \gamma'(\pi a),$$

où π est une uniformisante de K . Mais (4) que, pour $u \in A_{nr} - \{1\}$, on a $\gamma'(\pi au) = -\gamma'(\pi a)$; les termes de la deuxième somme se détruisent donc deux-à-deux. Enfin, dans la première somme, $\gamma'(a) = \gamma'(au)$ si $u \in A_{nr}$ et $a \in U$, d'où l'énoncé du lemme 1.

Si $p \neq 2$, on a $B = 1$ et $|A| = 4$, donc la démonstration est terminée. Supposons $p = 2$; posons $S = \sum_{a \in B} \gamma'(a)$. Pour $a \in U$, la forme bilinéaire symétrique $(x, y) \mapsto \text{Tr}(axy/\delta)$ est unimodulaire sur O_K ; par conséquent, on a par définition:

$$\gamma'(a) = (O_K : 2O_K)^{-1/2} \sum_{x \in O_K/2O_K} i^{-\text{Tr}(ax^2/\delta)}.$$

Soit \tilde{B} un système de représentants de B dans U . Considérons l'application:

$$f: \tilde{B} \times O_K/2O_K \rightarrow O_K/4O_K \\ (a, x) \mapsto ax^2 \pmod{4O_K}.$$

Comme les éléments de A_{nr} sont représentés par des éléments de $1 + 4O_K$, l'image de f n'est autre que $\bigcup_{0 \leq \alpha \leq e} T_{2\alpha}$, où e est l'indice de ramification absolu de K et $T_\alpha = \{y \in O_K \mid v(y) = \alpha\} \pmod{4O_K}$. Si $\alpha < e$ et $y \in T_{2\alpha}$, alors $f(a, x) = f(a', x') = y$ si et seulement si $a = a'$ et $x^2 \equiv x'^2 \pmod{4O_K}$; comme $v(x) =$

$v(x') = \alpha$, ceci signifie que $x' = tx$, avec $t^2 \equiv 1 \pmod{4O_K}$, donc toutes les fibres de f au dessus de $T_{2\alpha}$ ont même cardinal.

LEMME 2. Pour $0 \leq \alpha \leq 2e$,

$$\sum_{y \in T_\alpha} i^{-\text{Tr}(y/\delta)} = \begin{cases} 1 & \text{si } \alpha = 2e \\ -1 & \text{si } \alpha = 2e - 1 \\ 0 & \text{sinon.} \end{cases}$$

En effet, on a

$$\sum_{y \in T_\alpha} i^{-\text{Tr}(y/\delta)} = \sum_{v(y) \geq \alpha} i^{-\text{Tr}(y/\delta)} - \sum_{v(y) > \alpha} i^{-\text{Tr}(y/\delta)}$$

(sommer modulo $4O_K$). Dans le membre de droite, les deux sommes représentent la somme des valeurs d'un caractère sur un groupe, qui est nulle sauf si le caractère est trivial; ceci n'arrive que lorsque $\alpha = 2e$.

Donc dans la somme S , il ne reste que les termes (a, x) tels que $ax^2 \equiv 0 \pmod{4O_K}$. Chacun de ces termes donne une contribution de 1 et il y en a $|B|$; cela termine la première démonstration du théorème 1.

Deuxième démonstration. On suppose démontré le théorème 1 pour $p \neq 2$; c'est la partie facile de la démonstration précédente (Conner a aussi une autre preuve).

Soit K un corps de nombres; si v est une place finie de K , on l'identifie à la valuation qu'elle définit. Si v est une place réelle de K , on note \leq_v l'ordre induit sur K par v . Enfin, si v est une place quelconque de K , on note K_v le complété de K en v .

Soit S un ensemble fini de places de K , contenant les places à l'infini. On note S_f l'ensemble des places finies de S , $O_S = \{x \in K \mid v(x) \geq 0 \text{ si } v \notin S\}$ l'anneau des S -entiers de K et $G(S) = \prod_{v \in S} K_v^*/K_v^{*2}$: c'est un groupe fini d'exposant 2, et on a un homomorphisme diagonal $O_S^*/O_S^{*2} \rightarrow G(S)$. Par le théorème des S -unités [3, p. 105, corollaire], on a $(O_S^*:O_S^{*2}) = 2^{n+r_1+r_2}$ où $n = |S_f|$ et r_1 (resp. r_2) est le nombre de places réelles (resp. complexes) de K .

Notons $K^+ = \{x \in K^* \mid x >_v 0 \forall v \text{ réelle et } v(x) \text{ pair } \forall v \text{ finie}\}$. Le groupe K^+/K^{*2} est fini: en effet, soit C_K le groupe des classes de K et ${}_2C_K$ le sous-groupe des éléments tués par 2. On définit un homomorphisme $K^+ \rightarrow {}_2C_K$ de la manière suivante: si $a \in K^+$, l'idéal fractionnaire (a) est par définition de la forme \mathcal{A}^2 , où \mathcal{A} est un idéal fractionnaire bien déterminé; l'image de a est la classe de \mathcal{A} dans

C_K . Ceci induit un homomorphisme $K^+/K^{*2} \rightarrow {}_2C_K$, de noyau O_K^+/O_K^{*2} , où $O_K^+ = K^+ \cap O_K^*$. Comme O_K^+/O_K^{*2} et ${}_2C_K$ sont finis, K^+/K^{*2} est fini.

Disons que l'ensemble S est *gros* si:

- a) S contient toutes les places dyadiques de K ;
- b) S contient toutes les places de K ramifiées sur \mathbb{Q} (il suffirait de prendre les v telles que $v(\mathcal{D}_K)$ soit impair, où \mathcal{D}_K est la différentielle absolue de K);
- c) pour tout $x \in K^+ - K^{*2}$, il existe $v \in S_f$ telle que x ne soit pas un carré dans K_v .

La finitude de K^+/K^{*2} implique que l'on peut trouver de tels S .

LEMME 3. *Supposons S gros. Alors $\Delta: O_S^*/O_S^{*2} \rightarrow G(S)$ est injective, et $|G(S)| = (O_S^*: O_S^{*2})^2$.*

Démonstration. L'injectivité de Δ résulte de la condition c). Soit $v \in S$: alors on a

$$(K_v^*: K_v^{*2}) = \begin{cases} 1 & \text{si } v \text{ est complexe;} \\ 2 & \text{si } v \text{ est réelle;} \\ 4 & \text{si } v \text{ est finie, non dyadique;} \\ 2^{n_v+2} & \text{si } v \text{ est dyadique et } n_v = [K_v: \mathbb{Q}_2]. \end{cases}$$

Les places complexes offrent à $G(S)$ une contribution totale de 1; les places réelles une contribution de 2^{r_1} ; les places finies non dyadiques une contribution de 4^{n_-} , où n_- est leur nombre; enfin les places dyadiques offrent une contribution de $2^{\sum n_v} \cdot 4^{n_+}$, où l'on somme sur toutes les places dyadiques de K (cf a)) et où n_+ est leur nombre. Mais $\sum n_v = [K: \mathbb{Q}] = r_1 + 2r_2$ et $n = n_+ + n_-$, donc:

$$|G(S)| = 2^{r_1} \cdot 4^{n_-} \cdot 2^{r_1+2r_2} \cdot 4^{n_+} = 2^{2r_1+2r_2+2n} = (O_S^*: O_S^{*2})^2.$$

A partir de maintenant, on suppose S gros. Pour $v \in S_f$, soit $w_v: K_v^*/K_v^{*2} \rightarrow \mathbb{Z}/4$ l'application définie précédemment; si v est une place réelle, posons $w_v(x) = -\frac{1}{2}$ si $x <_v 0$, $w_v(x) = 0$ si $x >_v 0$: ceci définit encore une application $w_v: K_v^*/K_v^{*2} \rightarrow \mathbb{Q}_2/\mathbb{Z}_2$, telle que $w_v(xy) - w_v(x) - w_v(y) = \frac{1}{2}(x, y)_v$, où $(,)_v$ est le symbole de Hilbert local en v .

Définissons une application $w: G(S) \rightarrow \mathbb{Q}_2/\mathbb{Z}_2$ par $w((x_v)_{v \in S}) = \sum_{v \in S} w_v(x_v)$. Il est clair que pour $(x_v), (y_v) \in G(S)$, on a $w((x_v y_v)) - w((x_v)) - w((y_v)) = \frac{1}{2} \sum_{v \in S} (x_v, y_v)_v$. L'application w définit donc un élément de $WQ(\mathbb{Q}_2, \mathbb{Z}_2)$ qui est évidemment égal à la somme des classes des w_v pour $v \in S$. Notons $H(S)$ l'image de O_S^*/O_S^{*2} dans $G(S)$.

LEMME 4. *La restriction de w à $H(S)$ est identiquement nulle; en particulier, la classe de w dans $WQ(\mathbb{Q}_2, \mathbb{Z}_2)$ est triviale.*

En effet, si χ est un caractère du groupe des classes d'idéales de K , notons, pour toute place v de K , χ_v sa restriction à K_v^* et $W_v(\chi) = W(\chi_v)$. (Pour la définition de $W(\chi_v)$ quand v est réelle, cf [5, p. 32, déf.].) On sait [5, p. 33, th. 2.3] que les $W_v(\chi)$ sont presque tous égaux à 1 et que $\prod W_v(\chi)$ est la constante de l'équation fonctionnelle de $L(\chi, s)$; cette constante est égale à 1 si χ est un caractère quadratique [6, p. 125]. Soit $a \in K^*$ et ρ_a le caractère quadratique tel que $(\rho_a)_v(x) = (a, x)_v$ pour toute place v et tout $x \in K_v^*$: alors $\prod W_v(\rho_a) = 1$; de plus, $W_v(\rho_a) = \rho_a(\mathcal{D}_v)$ si v est finie, nondyadique et $a \in U_v$ (U_v : unités de K_v , \mathcal{D}_v différente absolue de K_v). En particulier, on a $W_v(\rho_a) = 1$ si $a \in O_S^*$ et $v \notin S$ (condition b) sur S), d'où la première affirmation du lemme 4. La deuxième en résulte grâce au lemme 3.

COROLLAIRE. *On a $\prod_{v \in S} \gamma(w_v) = 1$.*

Cela résulte du lemme 4 et de l'additivité de γ .

Fin de la démonstration. Soit maintenant K une extension finie de \mathbb{Q}_2 . D'après [3, p. 44, cor. à la prop. 4], il existe un corps de nombres $E \subset K$ tel que $[E:\mathbb{Q}] = [K:\mathbb{Q}_2]$ et que E soit dense dans K . En particulier, E n'a qu'une place dyadique v_0 et $E_{v_0} = K$. Notons $Q_E = Q = \text{Tr}_{E/\mathbb{Q}} x^2$; alors pour toute place l de \mathbb{Q} , Q_l ($:= Q \otimes_{\mathbb{Q}} \mathbb{Q}_l$) est la somme des Q_{E_v} , où v décrit les places divisant l . Par réciprocité de Weil [7, p. 179, prop. 5], on a:

$$\prod_l \gamma(Q_l) = \prod_v \gamma(Q_{E_v}) = 1. \quad (5)$$

Soit v une place finie, non dyadique de E ; on a supposé connu que $\gamma(w_v) = \gamma(Q_{E_v})$. Si v est une place infinie, la même formule se vérifie trivialement. La formule (5) et le corollaire au lemme 4 entraînent donc que $\gamma(w_{v_0}) = \gamma(Q_{E_{v_0}})$.

Transformée de Fourier. Le nombre $\overline{\gamma(w)}$ peut s'interpréter comme la valeur en 1 de la transformée de Fourier de W . Plus précisément, soit A' le groupe des caractères quadratiques de K , dual de $A = K^*/K^{*2}$. Munissons A et A' de la mesure de Haar de volume total $|A|^{1/2} = |A'|^{1/2}$. Alors la transformée de Fourier de W est par définition:

$$\hat{W}(x) = |A'|^{-1/2} \sum_{\rho \in A'} W(\rho) \rho(x) = |A|^{-1/2} \sum_{a \in A} W(\rho_a) (-1)^{(a,x)}.$$

THEOREME 2. Pour tout $x \in A$, on a $\hat{W}(x) = \overline{\gamma(x)}$.

Démonstration. Pour $x = 1$, c'est le théorème 1. Pour x quelconque, on calcule:

$$\begin{aligned} \hat{W}(x)\hat{W}(1) &= |A|^{-1} \sum_{(a,b) \in A^2} W(\rho_a)W(\rho_b)(-1)^{(a,x)} \\ &= |A|^{-1} \sum_{(a,b) \in A^2} W(\rho_{ab})(-1)^{(a,bx)} \quad (\text{formule (1)}) \\ &= |A|^{-1} \sum_{(a,c) \in A^2} W(\rho_c)(-1)^{(a,acx)} \\ &= |A|^{-1} \sum_{(a,c) \in A^2} W(\rho_c)(-1)^{(a,-cx)}. \end{aligned}$$

Si $-cx \neq 1$, on a $\sum_{a \in A} (-1)^{(a,-cx)} = 0$: en effet, le symbole de Hilbert est non-dégénéré. On trouve donc:

$$\hat{W}(x)\hat{W}(1) = |A|^{-1} \sum_{c \in A} W(\rho_c) \sum_{a \in A} (-1)^{(a,-cx)} = W(\rho_{-x}) = \gamma(-x)\gamma(1)^{-1}.$$

Comme $\hat{W}(1) = \overline{\gamma(1)} = \gamma(1)^{-1}$, on trouve $\hat{W}(x) = \gamma(-x) = \overline{\gamma(x)}$ (additivité de γ).

Caractères non quadratiques. Je vais calculer, dans le cas modéré, la transformée de Fourier de la restriction de W aux caractères d'ordre n (cas modéré: on suppose n premier à p). J'ignore si ces calculs ont un intérêt autre que de mettre en relief la spécificité du cas $n = 2$. Il serait intéressant de faire ce calcul également, disons, dans le cas $n = p$, mais cela paraît plus difficile.

THEOREME 3. Soit n un entier premier à p et $X_n = X_n(K)$ le groupe des caractères de K d'ordre n : c'est le dual de $A_n = K^*/K^{*n}$. Munissons X_n et A_n des mesures de Haar de volume total $|A_n|^{1/2} = |X_n|^{1/2}$. Alors la transformée de Fourier de W (restreint à X_n) a pour valeurs:

$$\hat{W}(a) = \begin{cases} 0 & \text{si } v(a) \not\equiv t, t+1 \pmod{n}; \\ \sqrt{n/r} & \text{si } v(a) \equiv t \pmod{n}; \\ \sqrt{n/qr} \sum_{u \in O_K/\mathcal{M}} e(\text{Tr}_{K/\mathbb{Q}_p} a^{-1}u^n) & \text{si } v(a) = t+1; \end{cases}$$

où l'on a noté $t = v(\mathcal{D}_K)$, $r = (n, q-1)$ et $e(x) = e^{2\pi i x}$.

Démonstration. Comme n est premier à p , tout élément de X_n se factorise par K^*/U_1 , donc est de conducteur 0 ou 1. On peut écrire $K^*/U_1 = \mathbb{Z} \times k^*$ (où k est le corps résiduel) au moyen d'une uniformisante de K . Par conséquent, K^*/K^{*n} s'écrit $\mathbb{Z}/n \times k^*/k^{*n}$; le premier facteur est cyclique d'ordre n tandis que le second est cyclique d'ordre r .

Dualement, on peut trouver une base (χ_0, χ_1) de χ_n , où χ_0 est un caractère non-ramifié d'ordre n et χ_1 un caractère ramifié (donc de conducteur 1) d'ordre r . Il en résulte, pour $a \in A_n$:

$$\hat{W}(a) = |A_n|^{-1/2} \sum_{\chi \in X_n} \chi(a)^{-1} W(\chi) = |A_n|^{-1/2} \sum_{\lambda, \mu} \chi_0(a)^{-\lambda} \chi_1(a)^{-\mu} W(\chi_0^\lambda \chi_1^\mu),$$

où (λ, μ) décrit $\mathbb{Z}/n \times \mathbb{Z}/r$. Rappelons la formule [6, p. 98, Cor.2]:

$$W(\chi\chi') = \chi(\mathcal{D}_{\chi'}) W(\chi'),$$

si χ est non-ramifié et $\mathcal{D}_{\chi'} = \mathcal{M}^{f(\chi')} \mathcal{D}_K$. On en déduit que:

$$\hat{W}(a) = |A_n|^{-1/2} \left[\sum_{\mu \neq 0} \chi_1(a)^{-\mu} W(\chi_1^\mu) \sum_{\lambda} \chi_0(x^{-1} \mathcal{M} \mathcal{D})^\lambda + \sum_{\lambda} \chi_0(x^{-1} \mathcal{D})^\lambda \right].$$

Si $v(a) \not\equiv t, t+1 \pmod{n}$, il est clair d'après cette formule que $\hat{W}(a) = 0$. De même, si $v(a) \equiv t \pmod{n}$, on voit que $\hat{W}(a) = |A_n|^{-1/2} n = \sqrt{n/r}$ puisque $|A_n| = nr$. Il reste le cas où $v(a) \equiv t+1 \pmod{n}$; on peut même supposer $v(a) = t+1$. Alors la formule ci-dessus devient:

$$\begin{aligned} \hat{W}(a) &= n |A_n|^{-1/2} \sum_{\mu \neq 0} \chi_1(a)^{-\mu} W(\chi_1^\mu) \\ &= n |A_n|^{-1/2} \sum_{\mu \neq 0} \chi_1(a)^{-\mu} q^{-1/2} \sum_{x \in U/U_1} \chi_1(d^{-1}x)^{-\mu} \psi_K(d^{-1}x) \\ &= n |A_n|^{-1/2} q^{-1/2} \sum_{x \in U/U_1} \psi_K(d^{-1}x) \sum_{\mu \neq 0} \chi_1(ad^{-1}x)^{-\mu} \\ &= n |A_n|^{-1/2} q^{-1/2} \left[\sum_{\substack{x \in U/U_1 \\ x \not\equiv a^{-1}d \pmod{U^n}}} (-\psi_K(d^{-1}x)) \right. \\ &\quad \left. + \sum_{\substack{x \in U/U_1 \\ x \equiv a^{-1}d \pmod{U^n}}} (r-1) \psi_K(d^{-1}x) \right] \\ &= n |A_n|^{-1/2} q^{-1/2} \left[r \sum_{\substack{x \in U/U_1 \\ x \equiv a^{-1}d \pmod{U^n}}} \psi_K(d^{-1}x) - \sum_{x \in U/U_1} \psi_K(d^{-1}x) \right]. \end{aligned}$$

On a $\sum_{x \in U/U_1} \psi_K(d^{-1}x) = -1$: c'est la somme sur $O_K/\mathcal{M} - \{0\}$ des valeurs d'un caractère non trivial de O_K/\mathcal{M} . Comme il y a r racines $n^{\text{ièmes}}$ de l'unité dans K^* , on en conclut après changement de variables:

$$\begin{aligned} \hat{W}(a) &= n |A_n|^{-1/2} q^{-1/2} \sum_{u \in O_K/\mathcal{M}} \psi_K(a^{-1}u^n) \\ &= \sqrt{n/qr} \sum_{u \in O_K/\mathcal{M}} e(\text{Tr}_{K/\mathbb{Q}_p} a^{-1}u^n) \end{aligned}$$

COROLLAIRE. Si $q = p$, on a $|\hat{W}(a)| \leq (r-1)\sqrt{n/r}$ lorsque $v(a) \equiv t+1 \pmod{n}$.

En effet, on peut alors trouver un $b \in \mathbb{F}_p^*$ tel que $p \text{Tr}_{K/\mathbb{Q}_p} a^{-1}u \equiv b\bar{u} \pmod{p}$, où \bar{u} est la réduction de u modulo \mathcal{M} ; le corollaire résulte alors de [1, p. 258, th. 8.5]. Par la même méthode on doit pouvoir établir le corollaire pour q quelconque.

(Je remercie Etienne Fouvry de m'avoir indiqué le résultat et la référence ci-dessus.)

Remarquons que dans l'énoncé du théorème 3, on peut remplacer les u^n par des u' .

EXEMPLES. a) $n = 3$. Si $r = 1$, on trouve d'après le théorème 3 et la remarque précédente:

$$\hat{W}(a) = \begin{cases} 0 & \text{si } v(a) \not\equiv t \pmod{3} \\ \sqrt{3} & \text{si } v(a) \equiv t \pmod{3}. \end{cases}$$

Si $r = 3$, prenons par exemple $K = \mathbb{Q}_7$: alors, si $v(a) = 1$, on obtient $\hat{W}(a) = 1/\sqrt{7}(1 + 3e(1/a) + 3e(-1/a))$, nombres algébriques totalement réels de degré 6 et de norme $-2^8/7^3$.

b) $n = 4$. Si $r = 2$, on trouve

$$\hat{W}(a) = \begin{cases} 0 & \text{si } v(a) \not\equiv t, t+1 \pmod{4} \\ \sqrt{2} & \text{si } v(a) \equiv t \pmod{4} \\ \sqrt{2} \gamma(a) & \text{si } v(a) \equiv t+1 \pmod{4}. \end{cases}$$

Si $r = 4$, prenons par exemple $K = \mathbb{Q}_5$. Alors si $v(a) = 1$, on obtient $\hat{W}(a) = 1/\sqrt{5}(1 + 4e(a^{-1}))$, nombres algébriques de degré 4 et de norme 41/5.

BIBLIOGRAPHIE

- [1] AYOUB, A., *An introduction to the analytic theory of numbers*, AMS, Providence, 1963.
- [2] KAHN, B., *Le groupe des classes modulo 2*, d'après Conner et Perlis, Sémin. th. nombres Bordeaux (1984–85), exposé n° 26.
- [3] LANG, S., *Algebraic number theory*, Addison–Wesley, Reading, 1970.
- [4] LANNES, J., *Formes quadratiques d'enlacement sur l'anneau des entiers d'un corps de nombres*, Ann. Sci. ENS 8 (1976), 535–579.
- [5] MARTINET, J., *Character theory and Artin L-functions*, in Algebraic number fields (A. Fröhlich, éd.), 1–88, Academic Press, New York, 1977.
- [6] TATE, J., *Local constants*, *ibid.*, 89–131.
- [7] WEIL, A., *Sur certains groupes d'opérateurs unitaires*, *Acta Math.* 111 (1964), 143–211.

Université de Paris 7
UFR de Mathématiques
5e étage, tour 45–55
75251 Paris Cedex 05 (France)

Reçu le 15 juillet 1986