Jean-Loup Waldspurger

Relèvement et formes quadratiques à 4 variables

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 18, n° 2 (1976-1977), exp. n° 25, p. 1-7
<http://www.numdam.org/item?id=SDPP_1976-1977__18_2_A6_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
18e année, 1976/77, n° 25, 7 p.

9 mai 1977

RELÈVEMENT ET FORMES QUADRATIQUES À 4 VARIABLES

par Jean-Loup WALDSPURGER

Cet exposé fait suite à un article de EICHLER : Theta functions over $\mathbb{Q}$ and over $\mathbb{Q}(\sqrt{q})$ [4], dans lequel il cherche à appliquer, aux formes quadratiques à 4 variables de discriminant premier q, les méthodes qu'il avait auparavant utilisées pour traiter le cas des formes de discriminant carré, en particulier, la construction des matrices de Brandt. Il obtient alors des résultats sur les formes de Hilbert sur $\mathbb{Q}(\sqrt{q})$ ainsi qu'une version "**series theta**" du relèvement de Doi-Naganuma. On résumera ici l'idée de la démonstration d'EICHLER, sous des hypothèses plus générales.

1. L'algèbre de Clifford.

Soient k un corps de nombres totalement réel, $\mathfrak{o}_k$ son anneau des entiers, et S un espace vectoriel de dimension 4 sur k muni d'une forme quadratique q. Son discriminant est bien défini dans $k^\times/k^{\times 2}$, et on suppose qu'il n'est pas un carré. On peut alors lui associer une extension quadratique K de k. Supposant que q est définie positive en toute place réelle de k, alors K est encore totalement réel. Notons $\delta_{K/k}$ le discriminant de l'extension K/k. Si L est un réseau de S, on peut définir la norme $q(L)$: c'est le $\mathfrak{o}_k$-module engendré par $\{q(a) ; a \in L\}$; et son déterminant $\delta(L)$: si L a une **base** sur $\mathfrak{o}_k$, c'est le $\mathfrak{o}_k$-module engendré par le déterminant de la matrice exprimant la forme q dans cette base, sinon c'est le produit des déterminants locaux de $L_\mathfrak{p}$ sur $k_\mathfrak{p}$ pour tous les idéaux premiers $\mathfrak{p}$ de $\mathfrak{o}_k$. L'hypothèse sera qu'il existe dans S un réseau L_0 de norme $q(L_0) = \mathfrak{o}_k$ et de déterminant $\delta(L_0) = \delta_{K/k}$. Un tel réseau est alors maximal, i. e. il n'existe pas de réseau de même norme le contenant strictement.

La **1re algèbre** de Clifford associée à S est le k-espace engendré par les suites $(a_1 \dots a_r)$ où $a_i \in S$, soumises aux relations de multilinéarité évidentes, et aux relations :

$$(ab) + (ba) = q(a + b) - q(a) - q(b) .$$

La multiplication est donnée par

$$(a_1 \dots a_r).(b_1 \dots b_s) = (a_1 \dots a_r\, b_1 \dots b_s) .$$

La 2e algèbre de Clifford C est la sous-algèbre engendrée par les suites $(a_1 \dots a_r)$ pour r pair. On montre que le centre de C est isomorphe à l'extension K, et que C est une algèbre de quaternions sur ce centre.

PROPOSITION. - L'algèbre de Clifford C est l'algèbre de quaternions sur K, définie, et non ramifiée en toute place finie (i. e. pour toute place réelle v de

K , C_v est isomorphe au corps des quaternions de Hamilton, et pour toute place finie, C_v est isomorphe à l'algèbre de matrices $M_2(K_v)$).

L'antiautomorphisme de C est défini par

$$(a_1 \dots a_{2r}) \longmapsto (a_{2r} \dots a_1) ,$$

on le note $M \mapsto \overline{M}$. Il laisse stable le centre K . On plonge S dans la 1re algèbre par $a \mapsto (a)$. Si $M \in C$ et $a \in S$, l'élément $\overline{M}(a) M$ est de la forme (b) pour un $b \in S$.

PROPOSITION. - L'application $a \mapsto b$, où $(b) = \overline{M}(a) M$, avec $M \in C$, est une similitude directe de S de norme $n_{K/k}(N_{C/K}(M))$. Réciproquement, pour toute similitude directe de S , il existe un $M \in C$ et un $t \in k$ tels que la similitude soit donnée par

$$a \longmapsto tb , \text{ où } (b) = \overline{M}(a) M$$

(on note $N_{C/K}(M) = M\overline{M} = \overline{M}M$).

On rappelle qu'un ordre de C est un réseau sur $\mathfrak{o}_k$ qui est un sous-anneau de C . Si L est un réseau de S , on peut lui associer un ordre $\mathcal{O}_L$ de C : c'est le $\mathfrak{o}_k$-module engendré par

$$\{t(a_1 \dots a_{2r}) \; ; \; a_i \in L \text{ et } t \in q(L)^{-r}\} .$$

On peut voir que $\mathcal{O}_L$ est maximal si, et seulement si, $q(L)$ est la norme $n_{K/k}(I)$ d'un idéal de K . En particulier, $\mathcal{O}_{L_0}$ est maximal. On se restreint aux réseaux L maximaux d'ordre associé maximal. Si $\mathfrak{M}$ est un $\mathcal{O}_L$-idéal à gauche (i. e. un réseau de C tel que $\mathcal{O}\mathfrak{M} = \mathfrak{M}$), on pose

$$\overline{\mathfrak{M}}(L)\, \mathfrak{M} = \{\sum t\overline{M}(a) M \; ; \; t \in \mathfrak{o}_k , \; M \in \mathfrak{M} \text{ et } a \in L\} .$$

THÉORÈME 1. - L'ensemble $L' = \overline{\mathfrak{M}}(L)\, \mathfrak{M}$ est un réseau maximal de S , d'ordre associé $\mathcal{O}_{L'}$ maximal. Cet ordre $\mathcal{O}_{L'}$ est l'ordre à droite de $\mathfrak{M}$. Réciproquement, si L et L' sont deux réseaux maximaux de S , d'ordres associés maximaux, il existe un idéal $\mathfrak{M}$ d'ordres à gauche $\mathcal{O}_L$ et à droite $\mathcal{O}_{L'}$ et un idéal m de k tels que $(L') = m\overline{\mathfrak{M}}(L)\, \mathfrak{M}$. On a l'égalité

$$q(L') = m^2\, n_{K/k}(N_{C/K}(\mathfrak{M}))\, q(L) .$$

De plus, si $(m_1 , \mathfrak{M}_1)$ et $(m_2 , \mathfrak{M}_2)$ vérifient les conditions précédentes, il existe un idéal I de K tel que $\mathfrak{M}_2 = \mathfrak{M}_1 I$ et $m_1 = n_{K/k}(I)\, m_2$.

(On note $N_{C/K}(\mathfrak{M})$ le $\mathfrak{o}_K$-module engendré par $\{N_{C/K}(M) \; ; \; M \in \mathfrak{M}\}$.)

2. Le théorème algébrique de relèvement.

On introduit les matrices de Brandt. Au-dessus d'une valuation réelle v de k , l'algèbre C_v est isomorphe au produit $\underline{H} \times \underline{H}$, où $\underline{H}$ désigne les quaternions de Hamilton. Fixons une fois pour toutes un nombre ℓ entier pair strictement positif.

Il est bien connu que $\underset{\sim}{H}^{\times}$ a essentiellement une seule représentation complexe irréductible de dimension $\ell + 1$. On en choisit une qu'on note r_ℓ . On en déduit une représentation $R_{\ell,v}$ de $C_v^{\times}$

$$C_v^{\times} \longrightarrow \underset{\sim}{H}^{\times} \times \underset{\sim}{H}^{\times} \longrightarrow GL((\ell+1)^2 , \underset{\sim}{C})$$

$$M \longmapsto (M_1 , M_2) \longmapsto r_\ell(M_1) \otimes r_\ell(M_2) .$$

Si $M \in C$, on pose $R_\ell(M) = \underset{v}{\otimes} R_{\ell,v}(M)$.

Soit $\mathcal{O}_{L_0}$ l'ordre maximal de C associé au réseau L_0 , et $(\mathfrak{M}_\alpha)_{\alpha=1\ldots h}$ un système de représentants des classes d'idéaux d'ordre à gauche $\mathcal{O}_{L_0}$ (deux idéaux $\mathfrak{M}$ et $\mathfrak{M}'$ sont équivalents s'il existe $M \in C$ tel que $\mathfrak{M} = \mathfrak{M}'M$). On note $\mathcal{O}_\alpha$ l'ordre à droite de $\mathfrak{M}_\alpha$ (ils ne sont pas tous distincts en général), et e_α le nombre d'éléments du quotient $\mathcal{O}_\alpha^{\times}/\mathfrak{o}_K^{\times}$. Pour I un idéal entier de K , on pose

$$\pi_{\alpha\beta}(I) = \textstyle\sum_M R_\ell(\overline{M})\, e_\beta^{-1} ,$$

où on somme sur les $M \in C$ tels que

(a) $\mathfrak{M}_\alpha^{-1}\,\mathfrak{M}_\beta\, M$ entier (i. e. $M \in \mathfrak{M}_\beta^{-1}\,\mathfrak{M}_\alpha$)

(b) $N_{C/K}(\mathfrak{M}_\alpha^{-1}\,\mathfrak{M}_\beta\, M) = I$,

(c) Dans un ensemble $\{\varepsilon M \; ; \; \varepsilon \in \mathfrak{o}_K^{\times}\}$, on ne prend qu'un élément (on vérifie qu'on a $R_\ell(\varepsilon M) = R_\ell(M)$).

La <u>matrice de Brandt</u> est alors la matrice à $h(\ell+1)^{2[k:\underset{\sim}{Q}]}$ lignes et colonnes :

$$B_\ell(I) = (\pi_{\alpha\beta}(I))_{\alpha,\beta=1\ldots h} .$$

Pour toute place réelle v de k , on fixe une base $(p_{\nu,v})_{\nu=1\ldots(\ell+1)^2}$ de l'espace des polynômes sphériques sur S_v pour la forme q , homogènes de degré ℓ . On pose $r = [k:\underset{\sim}{Q}]$. Si L est un réseau de S , n un idéal de k , et $\nu = (\nu_1 \ldots \nu_r) \in \{1 \ldots (\ell+1)^2\}^r$, on pose

$$m_\ell^0(\nu , n , L) = \textstyle\sum_a \left(\prod_{i=1}^{r} p_{\nu_i,v_i}(a)\right) ,$$

où on somme sur les $a \in L$ tels que $q(a)\,\mathfrak{o}_k = nq(L)$.

Soit $(h_i)_{i=1\ldots\varkappa}$ un système de représentants des classes d'idéaux du corps k . Notons, pour n un idéal de k , $|n| = n_{k/\underset{\sim}{Q}}(n)^{-1}$. On pose

$$m_\ell(\nu , n , L) = \textstyle\sum_{i=1}^{\varkappa} |h_i|^{\ell}\, m_\ell^0(\nu , n , h_i L) .$$

On définit la matrice colonne à $(\ell+1)^{2r}$ lignes :

$$m_\ell(n , L) = (m_\ell(\nu , n , L))_{\nu\in\{1\ldots(\ell+1)^2\}^r} .$$

Posons enfin $L_\alpha = \overline{\mathfrak{M}}_\alpha(L_0)\,\mathfrak{M}_\alpha$. On définit la matrice colonne à $h(\ell+1)^{2r}$ lignes.

$$m_\ell(n) = (m_\ell(n , L_\alpha))_{\alpha=1\ldots h} .$$

Ces matrices ont pour coefficients des coefficients de séries thêta sur k .

Si $\mathfrak{p}$ est un idéal premier de k , on définit les opérateurs de Hecke

$$T_{\mathfrak{p}}\, m_{\ell}(n) = m_{\ell}(n\mathfrak{p}) + |\mathfrak{p}|^{-(\ell+1)}\, m_{\ell}(n\mathfrak{p}^{-1}) ,$$

$$T_{\mathfrak{p}^2}\, m_{\ell}(n) = m_{\ell}(n\mathfrak{p}^2) + |\mathfrak{p}|^{-2(\ell+1)}\, m_{\ell}(n\mathfrak{p}^{-2}) - |\mathfrak{p}|^{-(\ell+1)}\, m_{\ell}(n) , \text{ si } \mathfrak{p} \text{ divise } n ,$$

$$= m_{\ell}(n\mathfrak{p}^2) \text{ si } \mathfrak{p} \text{ ne divise pas } n .$$

C'est une transcription de la définition classique.

THÉORÈME 2. - On peut trouver des bases $(p_{\nu,v})$ des polynômes sphériques telles que

(a) Si $\mathfrak{p}$ est un idéal premier de k , décomposé en $\mathfrak{P}_1 . \mathfrak{P}_2$ dans K , on a l'égalité

$$T_{\mathfrak{p}}\, m_{\ell}(n) = \frac{1}{2}\, [B_{\ell}(\mathfrak{P}_1) + B_{\ell}(\mathfrak{P}_2)] m_{\ell}(n) .$$

(b) Si $\mathfrak{p}$ est premier à $\delta_{K/k}$ et ne se décompose pas dans K , on a l'égalité

$$B_{\ell}(\mathfrak{p})\, m_{\ell}(n) = T_{\mathfrak{p}^2}\, m_{\ell}(n) + |\mathfrak{p}|^{-(\ell+1)}\, m_{\ell}(n) .$$

Autrement dit, la correspondance établie par le théorème 1 entre réseaux de S et idéaux de C transforme les opérateurs de Hecke en les matrices de Brandt. Il est à noter qu'on n'a pas, semble-t-il, de résultat analogue pour des matrices m_{ℓ}^{0} : on est forcé de faire intervenir les classes d'idéaux du corps k .

3. Expression analytique du relèvement.

On suppose $k = \mathbb{Q}$. Les hypothèses reviennent alors à se donner un nombre Δ_1 positif et sans carrés, à poser $\Delta = \Delta_1$ si $\Delta_1 \equiv 1 \mod 4$, $\Delta = 4\Delta_1$ si $\Delta_1 \equiv 2$ ou $3 \mod 4$, et à se donner une matrice carrée F à 4 lignes et 4 colonnes, entière, symétrique et paire, de déterminant Δ , et définissant une forme définie positive. On a $K = \mathbb{Q}(\sqrt{\Delta})$.

On a encore besoin de tenir compte du fait que le nombre de classes de K n'est pas supposé être égal à 1 , ce qui nous oblige à modifier la définition des matrices de Brandt. Soit toujours $\mathcal{O}_{L_0}$ l'ordre maximal de C associé au réseau L_0 et $(\mathcal{O}_{\alpha})_{\alpha=1\ldots h'}$ un système de représentants des classes d'ordres maximaux de C , pour l'équivalence donnée par les automorphismes intérieurs de C . Soit $\mathfrak{M}_{\alpha}$ un idéal d'ordre à gauche $\mathcal{O}_{L_0}$ et à droite $\mathcal{O}_{\alpha}$, et $(I_k)_{k=1\ldots\varkappa'}$ un système de représentants des classes d'idéaux de K . On peut trouver des sous-ensembles $\mathcal{C}_{\alpha} \subset \{1 \ldots \varkappa'\}$, tels que $(\mathfrak{M}_{\alpha} I_i)_{i\in\mathcal{C}_{\alpha}, \alpha=1\ldots h'}$ soit un système de représentants des classes d'idéaux de C . Le cardinal $|\mathcal{C}_{\alpha}|$ ne dépend pas du système choisi. Pour $\mathfrak{M}$ un idéal de C d'ordre à droite $\mathcal{O}_{\beta}$ et I un idéal de K , on pose :

$$\pi^{0}(\mathfrak{M} , I) = \sum_{M} R_{\ell}(\overline{M})\; e_{\beta}^{-1},$$

où on somme sur le même ensemble de M que précédemment (en remplaçant $\mathfrak{M}_\beta^{-1}\,\mathfrak{M}_\alpha$ par $\mathfrak{M}$). On définit la <u>matrice de Brandt réduite</u> :

$$B'_\ell(I) = (\pi'_{\alpha\beta}(I))_{\alpha,\beta=1\ldots h'} ,$$

avec $\pi'_{\alpha\beta}(I) = \dfrac{|C_\beta|}{\kappa'} \sum_{k=1}^{\kappa'} |I_k|^\ell\, \pi^0(\mathfrak{M}_\beta^{-1}\,\mathfrak{M}_\alpha\, I_k\,,\, I)$.

(On pourrait aussi faire intervenir des caractères du groupe des classes (I_k) .)

Ces matrices réduites vérifient les mêmes propriétés de multiplicativité que les opérateurs de Hecke (sur les formes de Hilbert sur K). De plus, elles diagonalisent toutes dans une même base.

On va utiliser la théorie adélique des formes automorphes (Cf. WEIL) pour définir des formes de Hilbert sur K . On note $\underset{\sim}{A}$ les adèles de K , $\underset{\sim}{I}$ les idèles, et $B_{\underset{\sim}{A}}$ le sous-groupe de $GL_2(\underset{\sim}{A})$:

$$B_{\underset{\sim}{A}} = \{\begin{pmatrix} x & y\\ 0 & 1\end{pmatrix};\quad y\in \underset{\sim}{A}\ ,\quad x\in \underset{\sim}{I}\} .$$

On note d la différente de $K/\underset{\sim}{Q}$, et ψ le caractère canonique de $\underset{\sim}{A}/K$. On définit une matrice de fonctions sur $B_{\underset{\sim}{A}}$, à valeurs dans $\underset{\sim}{C}$:

$$F(\begin{pmatrix} x & y\\ 0 & 1\end{pmatrix}) = \sum_{\substack{\xi\in K^\times\\ \xi x \text{ totalement } >0}} B'_\ell(\mathrm{div}(\xi\, dx))\ |x|^{(\ell+2)/2} \exp(-2\pi(\xi_1\, x_1 + \xi_2\, x_2))\ \psi(\xi y) ,$$

où ξ_1 , ξ_2 , x_1 , x_2 sont les images de ξ et x dans les deux complétés réels de K . On montre alors que F se prolonge sur $GL_2(\underset{\sim}{A})$ en une matrice Θ de formes automorphes paraboliques de poids $\ell + 2$, de niveau 1 et sans caractère.

On sait définir, pour $\mathfrak{P}$ un idéal premier de K , un opérateur de Hecke $\mathbf{T}_{\mathfrak{P}}$ agissant sur les formes de Hilbert (Cf. WEIL).

PROPOSITION. - <u>On a l'égalité</u>

$$\mathbf{T}_{\mathfrak{P}}\,\Theta = B'_\ell(\mathfrak{P})\ \Theta .$$

On définit comme précédemment les réseaux $L_\alpha = \overline{\mathfrak{M}}_\alpha(L_0)\,\mathfrak{M}_\alpha$, et pour $n\in\underset{\sim}{N}$, une matrice colonne $m_\ell(n)$ à $h'.(\ell + 1)^2$ lignes. Pour $\tau\in\underset{\sim}{C}$, $\mathrm{Im}(\tau) > 0$, on pose :

$$\vartheta(\tau) = \sum_{n=0}^{\infty} m_\ell(n)\ \exp(2\pi i n\tau) .$$

Les coefficients de cette matrice sont des formes modulaires paraboliques pour $\Gamma_0(\Delta)$, de poids $\ell + 2$ et de caractère $(\Delta/\circ)$.

Soit A une matrice carrée telle que $A^{-1}\,B'_\ell(\mathfrak{P})\,A$ soit diagonale pour tout $\mathfrak{P}$. On vérifie que $A^{-1}\,\Theta A$ est diagonale :

$$A^{-1}\,\Theta A = \mathrm{diag}(\Theta_i)_{i=1\ldots h'(\ell+1)^2} .$$

On pose

$$A^{-1}\,\vartheta(\tau) = (\vartheta_i(\tau))_{i=1\ldots h'(\ell+1)^2} .$$

D'après les résultats obtenus, Θ_i est fonction propre de tous les T_p, et ϑ_i est fonction propre de T_p si p se décompose dans K (i. e. $(\Delta/p) = 1$), et de T_{p^2} si p ne se décompose pas (i. e. $(\Delta/p) = -1$). On sait que l'espace des formes paraboliques pour $\Gamma_0(\Delta)$ de poids $\ell + 2$ et de caractère $(\Delta/\cdot)$ admet une base de fonctions propres pour tous les T_p. Soit (f_j) une telle base, et choisissons f_i un élément de base intervenant dans la décomposition de ϑ_i relativement à cette base (si $\vartheta_i \neq 0$). Posons enfin

$$\tilde{f}_i = f_i \big|_{\ell+2} \begin{pmatrix} 0 & -1 \\ \Delta & 0 \end{pmatrix} ,$$

i. e. $\tilde{f}_i(\tau) = f_i(-\frac{1}{\Delta\tau}) (\sqrt{\Delta}\,\tau)^{-(\ell+2)}$.

THÉORÈME 3. - Soient $Z_i(s)$, $\zeta_i(s)$, $\tilde{\zeta}_i(s)$ les séries de Dirichlet normalisées associées à Θ_i, f_i et $\tilde{f}_i$, pour $s \in \mathbb{C}$. Supposons que i est tel que $\vartheta_i \neq 0$ et Θ_i soit invariant par l'automorphisme de Galois de $K/\mathbb{Q}$. Alors on a

$$Z_i(s) = \zeta_i(s)\, \tilde{\zeta}_i(s) .$$

Pour terminer, remarquons qu'on peut se poser deux problèmes.

1° Caractériser les i tels que $\vartheta_i = 0$. On semble assez loin de résoudre cette question.

2° L'espace engendré par les séries thêta ϑ_i et $\tilde{\vartheta}_i$ est-il stable par les opérateurs de Hecke T_p si $(\Delta/p) = -1$? Pour démontrer le théorème 3, on est sorti de cet espace en introduisant la fonction f_i. La seule chose que je sache faire est que le choix de la fonction f_i intervenant dans ϑ_i ne modifie pas le théorème. En effet, on a le résultat suivant.

PROPOSITION. - Si deux éléments f_i et f'_i interviennent dans la décomposition de ϑ_i, alors ou bien $f_i = f'_i$, ou bien $f_i = \tilde{f}'_i$.

Cela découle d'un résultat de DELIGNE sur les représentations ℓ-adiques qui permet de montrer la proposition suivante.

PROPOSITION. - Si f et f' sont deux formes modulaires paraboliques de poids k sur $\Gamma_0(\Delta)$ de caractère $(\Delta/\cdot)$, propres pour tous les T_p, de valeurs propres $a(p)$, $a'(p)$ et si $a(p) = a'(p)$ pour $(\Delta/p) = 1$, alors $f = f'$ ou $f = \tilde{f}'$.

BIBLIOGRAPHIE

[1] DELIGNE (P.) et SERRE (J.-P.). - Formes modulaires de poids 1, Ann. scient. Ec. Norm. Sup., 4e Série, t. 7, 1974, p. 507-530.

[2] EICHLER (M.). - Quadratische Formen und orthogonale Gruppen. - Berlin, Springer-Verlag, 1952 (Grundlehren der mathematischen Wissenschaften, 63).

[3] EICHLER (M.). - The basis problem for modular forms, ... , "Modular functions of one variable, I", p. 75-151. - Berlin, Springer-Verlag, 1973 (Lecture

Notes in Mathematics, 320).

[4] EICHLER (M.). - Theta functions over $\mathbb{Q}$ and over $\mathbb{Q}(\sqrt{q})$ (non publié).

[5] WEIL (A.). - Dirichlet series and automorphic forms. - Berlin, Springer-Verlag, 1971 (Lecture Notes in Mathematics, 189).

(Texte reçu le 22 juin 1977)

Jean-Loup WALDSPURGER
9 rue Victor Considérant
75014 PARIS