ACTA ARITHMETICA
XXXVI (1980)

Formes quadratiques à 4 variables et relèvement

par

J.-L. WALDSPURGER (Paris)

Introduction. Dans son livre *Quadratische Formen und orthogonale Gruppen* [4], Eichler a découvert l'importance pour l'étude des formes quadratiques entières de certaines matrices de similitudes (généralisant les matrices définies par Brandt en 1943 dans le cas des quaternions). Ces matrices de similitudes possèdent de remarquables propriétés de multiplication, analogues aux propriétés de multiplication des opérateurs de Hecke dans les espaces de formes modulaires. Les récents théorèmes de relèvement (dits de „lifting") des formes automorphes, dus en particulier à Naganuma, ont apporté des idées nouvelles pour l'étude des formes quadratiques entières. Guidé par les méthodes de lifting, Eichler a exposé à Bonn (Conférence on modular forms 1976) un cas particulier de relèvement de réseaux qui reflète en termes de formes quadratiques les résultats obtenus par Naganuma.

Dans cet article, nous allons redonner un exposé des travaux d'Eichler en les présentant dans un cadre plus général. Nous avons voulu présenter une exposition détaillée et complète des résultats, au risque de la rendre un peu longue. On part d'un espace vectoriel S de dimension 4 sur un corps de nombres totalement réel k, muni d'une forme quadratique totalement anisotrope dont le discriminant δ, bien défini dans $k^\times/k^{\times 2}$ n'est pas un carré. On introduit sa deuxième algèbre de Clifford C, qui est l'unique corps de quaternions totalement défini sur $K = k(\sqrt{\delta})$, de discriminant 1. On étudie les réseaux entiers de S dont le déterminant est égal au discriminant de K/k. Il est possible d'établir une correspondance entre ces réseaux de S et les idéaux de C, compatible avec les opérations données par les matrices de similitudes de Eichler. Par l'intermédiaire des séries thêta (qui sont ici les formes modulaires holomorphes associées à une forme quadratique définie positive et à un polynôme sphérique), la correspondance ci-dessus se transforme en l'application de Naganuma (pour $k = \mathbb{Q}$).

I. Résumé des résultats

1. 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. On suppose 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 définit sa norme $q(L)$: c'est l'idéal fractionnaire de k engendré par $\{q(a); a \in L\}$. On définit son déterminant $\delta(L)$: si L a une base sur $\mathfrak{o}_k$, c'est l'idéal fractionnaire 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 $\mathfrak{o}_k$. *On suppose qu'il existe dans S un réseau L_0 de norme $q(L_0) = \mathfrak{o}_k$ et de déterminant $\delta(L_0) = \delta_{K/k}$.* On explicitera plus loin ces hypothèses quand $k = \boldsymbol{Q}$.

2. On introduit la deuxième algèbre de Clifford C associée a l'espace S. C'est une algèbre de quaternions sur son centre, lequel est isomorphe à K. L'algèbre C est totalement définie, et non ramifiée en toute place finie. D'autre part, on peut associer à chaque élément de C une similitude directe de l'espace S. On établira alors une certaine correspondance entre les réseaux de l'espace S et les idéaux de l'algèbre C. Plus précisément on associe au réseau L_0 un ordre maximal $\mathfrak{O}_0$ de C. Si $(\mathfrak{M}_a)$ pour a variant de 1 à h, désigne un système de représentants des classes d'idéaux de C d'ordre à gauche $\mathfrak{O}_0$, on associera à chaque $\mathfrak{M}_a$ un réseau L_a de S. Fixons un entier l pair strictement positif. On sait construire, pour chaque idéal I de l'anneau des entiers $\mathfrak{o}_K$ de K, une matrice de Brandt $B_l(I)$. C'est une matrice carrée qui exprime l'opérateur de Hecke T_I dans un espace de formes automorphes sur K [5]. D'autre part, on saura introduire une certaine base de polynômes sphériques de degré l sur l'espace S, et associer ainsi à chaque réseau L_a et chaque idéal n de $\mathfrak{o}_k$ une matrice colonne $m_l(L_a, n)$, dont les termes sont des coefficients de séries thêta sur k. On définit la matrice colonne:

$$m_l(n) = (m_l(L_a, n)) \quad \text{pour } a \text{ variant de } 1 \text{ à } h.$$

Pour tout idéal r de $\mathfrak{o}_k$, on peut définir l'action de l'opérateur de Hecke T_r sur les matrices $m_l(n)$. Le résultat central est alors:

THÉORÈME. *Si $\mathfrak{p}$ est un idéal premier de $\mathfrak{o}_k$, premier à $\delta_{K/k}$, on a:*
(a) *si $\mathfrak{p}$ se décompose dans K en $\mathfrak{p} = \mathfrak{P}_1 \cdot \mathfrak{P}_2$,*

$$\tfrac{1}{2}[B_l(\mathfrak{P}_1) + B_l(\mathfrak{P}_2)]m_l(n) = T_\mathfrak{p} m_l(n),$$

(b) *si $\mathfrak{p}$ est inerte dans K,*

$$B_l(\mathfrak{p})m_l(n) = T_{\mathfrak{p}^2} m_l(n) + |\mathfrak{p}|^{-(l+1)} m_l(n).$$

Par la suite, on aura besoin de modifier un peu les matrices de Brandt et les matrices $m_l(n)$, en liaison avec le fait que les idéaux de k et K ne sont pas supposés tous principaux. Ces matrices de Brandt modifiées seront diagonalisables, toutes dans une même base.

3. Pour obtenir l'interprétation analytique du théorème précédent, on supposera $k = \boldsymbol{Q}$. Les hypothèses reviennent alors à choisir un nombre Δ_1 sans carrés, positif. On pose $\Delta = \Delta_1$ si $\Delta_1 \equiv 1 \bmod 4$, $\Delta = 4\Delta_1$ si $\Delta_1 \equiv 2, 3 \bmod 4$. Si Q est une matrice carrée entière de rang 4, symétrique et paire, définie positive, de déterminant Δ, on pose, pour $\tau \in \boldsymbol{C}, \operatorname{Im}\tau > 0$:

$$\vartheta(\tau) = \sum m_l(n) e^{2\pi i n\tau}, \quad \text{pour } n \text{ allant de } 0 \text{ à } \infty.$$

Ses coefficients sont des formes modulaires paraboliques de poids $l+2$ pour $\Gamma_0(\Delta)$, de caractère le caractère résiduel $(\Delta/\cdot)$. Le théorème implique que l'espace des séries thêta engendré par les coefficients de $\vartheta(\tau)$ est stable par les opérateurs de Hecke T_p si p est premier et $(\Delta/p) = 1$, et par T_{p^2} si $(\Delta/p) = -1$. D'autre part, en utilisant la théorie adélique des formes automorphes, on peut définir une matrice Φ_1 de formes de Hilbert pour K, à partir des matrices de Brandt (de la même façon que les $m_l(n)$ fournissent la matrice $\vartheta(\tau)$). On a, pour tout idéal premier $\mathfrak{P}$ de $\mathfrak{o}_K$, l'égalité: $T_\mathfrak{P}\Phi_1 = B_l(\mathfrak{P})\Phi_1$. Diagonalisons les matrices de Brandt modifiées. La matrice Φ_1 se transforme en une matrice Θ diagonale. On pose $\Theta = \operatorname{diag}(\Theta_i)$. La matrice colonne ϑ se transforme en une matrice colonne (ϑ_i). Les Θ_i sont des formes de Hilbert propres pour tous les opérateurs de Hecke. On peut montrer qu'elles engendrent l'espace des formes de Hilbert. La difficulté est que ϑ_i d'une part peut être nul, d'autre part est propre pour T_p si $(\Delta/p) = 1$, mais seulement pour T_{p^2} si $(\Delta/p) = -1$. Si ϑ_i est non nul, on pourra associer à ϑ_i un couple unique $(f_i, \tilde{f}_i)$ de formes paraboliques propres pour tous les opérateurs de Hecke vérifiant

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

Soient $Z_i(s)$, $\zeta_i(s)$, $\tilde{\zeta}_i(s)$ les séries de Dirichlet associées à Θ_i, f_i, $\tilde{f}_i$. On a alors:

THÉORÈME. *Si i est tel que $\vartheta_i \neq 0$ et que Θ_i soit invariant par l'action de $\operatorname{Gal}(K/\boldsymbol{Q})$, alors pour $s \in \boldsymbol{C}$, on a l'égalité:*

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

C'est la forme du théorème de Naganuma [8].

II. Réseaux et algèbre de Clifford

1. On se place dans les hypothèses de I.1. Quand on choisira une base de l'espace S, on notera Q la matrice de la forme q dans cette base (si $a \in S$ et si A est la matrice colonne des coordonnées de a dans la base en question, on a $q(a) = \frac{1}{2}{}^tAQA$). Pour tout idéal premier $\mathfrak{p}$ de $\mathfrak{o}_k$ et tout $\mathfrak{o}_k$-module X, on note $X_\mathfrak{p}$ le complété de X en $\mathfrak{p}$.

PROPOSITION 1. *Soit $L_\mathfrak{p}$ un réseau de $S_\mathfrak{p}$, entier $(q(L_\mathfrak{p}) \subset \mathfrak{o}_\mathfrak{p})$, et soit $K_\mathfrak{p} = k_\mathfrak{p}(\sqrt{\det L_\mathfrak{p}})$. Alors le discriminant $\delta(K_\mathfrak{p}/k_\mathfrak{p})$ divise $\delta(L_\mathfrak{p})$.*

COROLLAIRE. *Le réseau L_0 est maximal* (i.e. il n'existe pas de réseau L' contenant strictement L_0 et tel que $q(L_0) = q(L')$).

En effet, L_0 est de discriminant minimal parmi tous les réseaux entiers.

Démonstration de la proposition. Si $\mathfrak{p}$ ne divise pas 2, elle est immédiate. Rappelons le résultat suivant ([4], p. 48):

PROPOSITION 2. *Si $\mathfrak{p}$ est un idéal premier de $\mathfrak{o}_k$,*

(a) *si $\mathfrak{p}$ ne divise pas 2, tout réseau de $S_\mathfrak{p}$ possède une base orthogonale,*

(b) *si $\mathfrak{p}$ divise 2, tout réseau $L_\mathfrak{p}$ de $S_\mathfrak{p}$ possède une base (e_i) dans laquelle la matrice Q de la forme q s'écrit:*

$$Q = \begin{pmatrix} 2u_1 & u_{12} & & 0 \\ u_{12} & 2u_2 & & \\ & & 2u_3 & u_{34} \\ 0 & & u_{34} & 2u_4 \end{pmatrix} \quad \text{avec} \quad u_{ij} \in q(L_\mathfrak{p}).$$

Soient alors $\mathfrak{p}$ un idéal premier divisant 2, π une uniformisante en $\mathfrak{p}$, et (e_i) une base de $L_\mathfrak{p}$ comme ci-dessus. On a les formules ([4], p. 36):

(a) $\delta(K_\mathfrak{p}/k_\mathfrak{p}) = 4\mathfrak{p}$ si la valuation $\mathfrak{p}$-adique de $\det(L_\mathfrak{p})$ est impaire,

(b) $\delta(K_\mathfrak{p}/k_\mathfrak{p}) = 4\mathfrak{p}^{-2g}$ si cette valuation est paire, où g est le plus grand entier tel que c soit un carré modulo $\mathfrak{p}^{2g}$, si c est une unité telle que $\det(L_\mathfrak{p}) = c\pi^v$.

On a $\det(L_\mathfrak{p}) = (4u_1u_2 - u_{12}^2)(4u_3u_4 - u_{34}^2)$. Si sa valuation est impaire, cela entraîne que soit u_{12}, soit u_{34} est divisible par 2. Alors $\det(L_\mathfrak{p})$ est divisible par 4, donc par $4\mathfrak{p}$ puisque sa valuation est impaire. Supposons au contraire la valuation de $\det(L_\mathfrak{p})$ paire. Si u_{12} ou u_{34} est divisible par 2, alors 4 divise $\det(L)$ et *à fortiori* $4\mathfrak{p}^{-2g}$ divise $\det(L_\mathfrak{p})$. Sinon on a:

$$\det(L_\mathfrak{p}) = u_{12}^2u_{34}^2(4u_1u_2u_{12}^{-2} - 1)(4u_3u_4u_{34}^{-2} - 1).$$

On peut poser:

$$c = (4u_1u_2u_{12}^{-2} - 1)(4u_3u_4u_{34}^{-2} - 1).$$

En inversant au besoin les couples (e_1, e_2) et (e_3, e_4), on a $c \equiv 1 \bmod 4u_{34}^{-2}\mathfrak{o}_\mathfrak{p}$. Donc $4u_{34}^{-2}\mathfrak{o}_\mathfrak{p}$ divise $\mathfrak{p}^{2g}$, ce qui implique que $4\mathfrak{p}^{-2g}$ divise u_{34}^2 et donc divise $\det(L_\mathfrak{p})$. ∎

En reprenant ce calcul pour $L_\mathfrak{p} = L_{0,\mathfrak{p}}$, auquel cas $\delta(L_{0,\mathfrak{p}}) = \delta(K_\mathfrak{p}/k_\mathfrak{p})$, on vérifie

LEMME 1. *Si $\mathfrak{p}$ divise 2, le réseau $L_{0,\mathfrak{p}}$ possède une base (e_i) comme dans la proposition 2, avec u_1, u_{12} et u_3 des unités de $\mathfrak{o}_\mathfrak{p}$.*

2. L'algèbre de Clifford. La 1ère algèbre 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 2ème algèbre C est la sous-algèbre engendrée par les suites $(a_1 \dots a_r)$ pour r pair. Prenons une base orthogonale (e_i) de S. On vérifie facilement que C est une algèbre de quaternions sur son centre, lequel est engendré par 1 et $(e_1e_2e_3e_4)$. Comme $(e_1 \dots e_4)^2 = (\det Q)/16$, ce centre est isomorphe à $K = k(\sqrt{\det Q})$. L'antiautomorphisme de C au-dessus de K, noté $M \mapsto \overline{M}$ est défini par $(a_1 \dots a_{2r}) \mapsto (a_{2r} \dots a_1)$, la norme réduite par $N_{C/K}(M) = M\overline{M} = \overline{M}M$.

PROPOSITION 3. *L'algèbre C est l'algèbre de quaternions sur K, totalement définie et non ramifiée en toute place finie de K.*

Démonstration. On vérifie facilement que les éléments 1, $I = (e_1e_2)$, $I_2 = (e_2e_3)$ et $I_3 = (e_1e_3)$ forment une base de C sur K, soumis aux relations: $I_1^2 = -\alpha$, $I_2^2 = -\beta$, $I_3^2 = -\gamma$, $I_iI_j = -I_jI_i$ pour $i \neq j$, avec $\alpha = q(e_1)q(e_2)$, $\beta = q(e_2)q(e_3)$, $\gamma = q(e_1)q(e_3)$. La norme réduite d'un élément $M = x_0 + x_1I_1 + x_2I_2 + x_3I_3$ est égale à

$$N_{C/K}(M) = x_0^2 + x_1^2\alpha + x_2^2\beta + x_3^2\gamma.$$

Les nombres α, β, γ sont totalement positifs car q est totalement anisotrope, donc C est un corps de quaternions totalement défini sur K.

Localement, si $\mathfrak{P}$ est un idéal premier de $\mathfrak{o}_K$ ne divisant pas 2, et si $\mathfrak{p}$ est l'idéal de $\mathfrak{o}_k$ sous $\mathfrak{P}$, on peut supposer que (e_i) est une base de $L_{0,\mathfrak{p}}$. Comme $\delta(K_\mathfrak{P}/k_\mathfrak{p}) = \mathfrak{o}_\mathfrak{p}$ ou $\mathfrak{p}\mathfrak{o}_\mathfrak{p}$, on peut se ramener à α, β, γ unités de $\mathfrak{o}_\mathfrak{p}$. La norme réduite de $C_\mathfrak{P}$ sur $K_\mathfrak{P}$ représente 0 ([1], p. 55), donc $C_\mathfrak{P} \approx M_2(K_\mathfrak{P})$.

Si $\mathfrak{P}$ divise 2, soit (f_i) une base de $L_{0,\mathfrak{p}}$ comme dans le lemme 1, et définissons la base orthogonale (e_i) de $S_\mathfrak{p}$: $e_1 = f_1$, $e_2 = f_2 - (u_{12}/2u_1)f_1$, $e_3 = f_3$, $e_4 = f_4 - (u_{34}/2u_3)f_3$. Alors la norme réduite d'un élément $M = x_0 + x_1I_1 + x_2I_2 + x_3I_3$ est égale à

$$N_{C/K}(M) = x_0^2 + x_1^2u_1[u_2 - (u_{12}^2/4u_1)] + x_2^2u_3[u_2 - (u_{12}^2/4u_1)] + x_3^2u_1u_3.$$

Posons $y_0 = 2x_0$, $y_1 = x_1$, $y_2 = x_2$, $y_3 = 2u_1x_3$. Alors:

$$P(y) = 4u_1N_{C/K}(M) = y_0^2u_1 + y_1^2u_1(4u_1u_2 - u_{12}^2) + y_2^2u_3(4u_1u_2 - u_{12}^2) + y_3^2u_3.$$

Cette expression a pour coefficients des unités de $\mathfrak{o}_\mathfrak{p}$. De plus l'équation $P(y) \equiv 0 \bmod (4\mathfrak{p})$ a des solutions non triviales. En effet, l'élévation au carré étant une bijection dans $\mathfrak{o}/\mathfrak{p}$, il existe une unité u telle que $u_1 \equiv u^2u_3 \bmod \mathfrak{p}$. Alors $y_0 = u_{12}$, $y_1 = 1$, $y_2 = u$, $y_3 = uu_{12}$ est une telle solution. Donc $P(y)$ représente 0 dans $K_\mathfrak{p}$([1], p. 56) et $C_\mathfrak{p} \approx M_2(K_\mathfrak{p})$. ∎

3. Similitudes. Soit $a \in S$ et $M \in C$. On peut construire l'élément $\overline{M}(a)M$ de la 1ère algèbre de Clifford. On vérifie qu'il est de la forme (b) pour un élément b de S, car la dimension de S est 4. On notera $b = \overline{M}(a)M$. L'élément M de C agit donc sur S par $a \mapsto \overline{M}(a)M$.

Proposition 4. *Toutes les similitudes directes de S sont données par: $a \mapsto t\,\overline{M}(a)M$, où t (resp. M) est un élément arbitraire non nul de k (resp. C). La norme de cette similitude est $t^2n_{K/k}N_{C/K}(M)$. De plus deux paires (t_1, M_1) et (t_2, M_2) définissent la même similitude si et seulement si il existe $\mu \in K$ tel que $M_2 = \mu M_1$ et $t_2 = n_{K/k}(\mu)^{-1}t_1$.*

Démonstration. Vérifions que $a \mapsto b = \overline{M}(a)M$ est une similitude directe. On a: $q(b) = (bb) = \overline{M}(a)M\overline{M}(a)M$. On a le lemme facile suivant:

Lemme 2. *Si $a \in S$, $a \neq 0$, l'application $M \mapsto (a)^{-1}M(a) = q(a)^{-1}(a)M(a)$ est un automorphisme de C induisant l'automorphisme σ galoisien non trivial de K/k sur le centre K de C.*

Alors, comme $M\overline{M} = N_{C/K}(M)$ est dans le centre, on a:

$$q(b) = \overline{M}N_{C/K}(M)^\sigma(aa)M = N_{C/K}(M)^\sigma N_{C/K}(M)q(a) = n_{K/k}N_{C/K}(M)q(a).$$

L'application est bien une similitude de la norme indiquée. D'autre part, il est clair que si τ est une similitude et (e_i) une base orthogonale de S, on a

$$(\tau e_1\tau e_2\tau e_3\tau e_4) = \det(\tau)(e_1e_2e_3e_4).$$

Grâce au lemme précédent, on peut calculer le membre de gauche pour $\tau(a) = \overline{M}(a)M$ et vérifier que cette similitude est directe.

Réciproquement, si τ est une similitude directe de norme $s \in k$, on sait que s est totalement positif, et qu'il existe $\mu \in K$ tel que $s = n_{K/k}(\mu)$ ([4], p. 65). Posons $\mu = x + y\sqrt{\Delta}$ avec x, $y \in k$ et $\Delta = \det Q$ en fixant une base. Alors $s = x^2 - y^2\Delta$. Puisque s est totalement positif, on a $x \neq 0$. La similitude $x\tau$ est de norme x^2s, de la forme $x^2s = n_{K/k}(x\mu)$ et $x\mu$ est un élément totalement positif de K. Un tel élément est de la forme $x\mu = N_{C/K}(M)$. Alors τ est le produit de la similitude $a \mapsto x^{-1}\overline{M}(a)M$ par un automorphisme direct de S. Le cas d'un automorphisme est traité dans [4], p. 26, d'où la conclusion. L'assertion d'"unicité" est évidente. ∎

On a bien sûr des propositions locales analogues.

4. Réseaux de S et idéaux de C. On renvoit à [5], p. 16 à 20, pour la théorie des ordres et idéaux dans une algèbre de quaternions.

Soit L un réseau maximal de S. On lui associe un sous-anneau $\mathfrak{O}_L$ de C: c'est le $\mathfrak{o}_k$-module engendré par les éléments $t(a_1 \dots a_{2r})$ avec $a_i \in L$ et $t \in q(L)^{-r}$. D'après [4], p. 98, si deux réseaux L, L' sont tels que $\mathfrak{O}_L = \mathfrak{O}_{L'}$ alors il existe un idéal m de k tel que $L' = mL$. Remarquons que pour $M \in \mathfrak{O}_L$ et $a \in L$, on a $\overline{M}(a)M \in L$ (la réciproque est fausse: il existe des M tels que $M \notin \mathfrak{O}_L$ et que $\overline{M}(L)M \subset L$).

Proposition 5. *Si L est un réseau maximal de S dont la norme $q(L)$ est la norme d'un idéal de K, alors son anneau associé $\mathfrak{O}_L$ est un ordre maximal de C.*

Démonstration. Elle est locale. On démontre d'abord la proposition pour L_0, où on note $\mathfrak{O}_0$ son anneau associé. Ce cas est traité dans [10], Satz 10, 11, si $k = \mathbf{Q}$, ce qui n'est pas vraiment restrictif, sauf au-dessus d'une place $\mathfrak{p}$ de $\mathfrak{o}_k$ divisant 2. Dans ce cas, soit (e_i) une base de $L_{0,\mathfrak{p}}$ fournie par le lemme 1. On introduit $\eta = (2(e_1e_2) - u_{12})(2(e_3e_4) - u_{34})$. Alors

$$\eta^2 = (4u_1u_2 - u_{12}^2)(4u_3u_4 - u_{34}^2) = \det Q, \quad \text{et} \quad K_\mathfrak{p} = k_\mathfrak{p}(\eta).$$

On vérifie classiquement que $\mathfrak{o}_{K_\mathfrak{p}} = \mathfrak{o}_{k_\mathfrak{p}}[1, (u_{12}u_{34} + \eta)/2]$. Or

$$\eta = 4(e_1e_2e_3e_4) - 2u_{34}(e_1e_2) - 2u_{12}(e_3e_4) + u_{12}u_{34}.$$

Alors $(u_{12}u_{34} + \eta)/2 \in \mathfrak{O}_{0,\mathfrak{p}}$, donc $\mathfrak{o}_{K_\mathfrak{p}} \subset \mathfrak{O}_{0,\mathfrak{p}}$. On peut localiser en un idéal $\mathfrak{P}$ de $\mathfrak{o}_K$ au-dessus de $\mathfrak{p}$. On considère le sous-module de $\mathfrak{O}_{0,\mathfrak{P}}$ suivant:

$$\mathfrak{o}_{K_\mathfrak{P}}[1, (e_1e_2), (e_2e_3), (e_1e_3)].$$

Son discriminant par rapport à $\mathfrak{o}_K$ est:

$$\det \begin{vmatrix} 2 & u_{12} & & 0 \\ u_{12} & 2u_1u_2 & & \\ & & 2u_3u_2 & u_3u_{12} \\ 0 & & u_3u_{12} & 2u_3u_1 \end{vmatrix} = (4u_1u_2 - u_{12}^2)^2u_3^2.$$

D'après le lemme 1, c'est une unité. Alors ce sous-module est $\mathfrak{O}_{0,\mathfrak{P}}$ tout entier et $\mathfrak{O}_{0,\mathfrak{P}}$ est maximal.

Deux réseaux semblables ont des anneaux associés conjugués par automorphisme intérieur (proposition 4). Il suffit pour terminer la démonstration de vérifier que $L_\mathfrak{p}$ est semblable à $L_{0,\mathfrak{p}}$. Comme $q(L_\mathfrak{p})$ est la norme d'un idéal de $K_\mathfrak{p}$ et que localement les idéaux sont principaux, il existe $\mu \in K_\mathfrak{p}$ tel que $q(L_\mathfrak{p}) = n_{K_\mathfrak{p}/k_\mathfrak{p}}(\mu)\mathfrak{o}_\mathfrak{p}$. Soit $M \in C_\mathfrak{p}$ tel que $\mu = N_{C_\mathfrak{p}/K_\mathfrak{p}}(M)$ et posons $L'_\mathfrak{p} = \overline{M}^{-1}(L_\mathfrak{p})M^{-1}$. Alors $q(L'_\mathfrak{p}) = \mathfrak{o}_\mathfrak{p}$. D'après [4], p. 26 et 52, $L_{0,\mathfrak{p}}$ est isomorphe à $L'_\mathfrak{p}$, et donc semblable à $L_\mathfrak{p}$. ∎

Enonçons maintenant le résultat principal de cette partie. Si L est un réseau d'anneau associé $\mathfrak{O}_L$ et si $\mathfrak{M}$ est un $\mathfrak{O}_L$-idéal à gauche de C, on pose:

$$\overline{\mathfrak{M}}(L)\mathfrak{M} = \left\{\sum \bar{M}(a)M;\ M \in \mathfrak{M},\ a \in L\right\}.$$

THÉORÈME 1. *Si L est un réseau maximal de S, d'ordre associé maximal $\mathfrak{O}_L$, soit $\mathfrak{M}$ un $\mathfrak{O}_L$-idéal à gauche de C et $L' = \overline{\mathfrak{M}}(L)\mathfrak{M}$. Alors L' est un réseau maximal de S d'ordre associé maximal égal à l'ordre à droite de $\mathfrak{M}$. On a*

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

Réciproquement si L et L' sont deux réseaux maximaux de S, d'ordres associés $\mathfrak{O}_L$ et $\mathfrak{O}_{L'}$ maximaux et soit $\mathfrak{M}$ un idéal d'ordre à gauche $\mathfrak{O}_L$ et à droite $\mathfrak{O}_{L'}$, il existe un idéal m de k tel que $L' = m\overline{\mathfrak{M}}(L)\mathfrak{M}$. Si $(\mathfrak{M}_1, m_1)$ et $(\mathfrak{M}_2, m_2)$ vérifient l'égalité précédente, alors il existe un idéal I de K tel que

$$\mathfrak{M}_2 = \mathfrak{M}_1 I \quad \text{et} \quad m_2 = n_{K/k}(I)^{-1}m_1.$$

COROLLAIRE. *Si L est un réseau maximal de S d'ordre associé maximal, alors $q(L)$ est la norme d'un idéal de K.*

Il suffit d'appliquer le théorème au couple L, L_0.

Démonstration du théorème. Elle est locale. Au dessus de k_p, tous les idéaux sont principaux. Alors $\overline{\mathfrak{M}}(L)\mathfrak{M} = \overline{M}\overline{\mathfrak{O}}_L(L)\mathfrak{O}_L M = \overline{M}(L)M$ pour un certain $M \in C_p$ et on en déduit facilement la première assertion (compte tenu de la proposition 4). La deuxième assertion résulte de la première et du fait que deux réseaux ayant même ordre associé ne diffèrent que par un idéal de k. Pour l'"unicité", on remarque que $\mathfrak{M}_2\mathfrak{M}_1^{-1}$ est un idéal bilatère. Donc il existe un idéal I de K tel que $\mathfrak{M}_2\mathfrak{M}_1^{-1} = \mathfrak{O}_L I$ ([5], p. 18). D'où $\mathfrak{M}_1 = \mathfrak{M}_2 I$ et l'assertion sur les m_i s'en déduit facilement. ■

III. Représentations de l'algèbre de Clifford

On va étudier la représentation inverse $a \mapsto \bar{M}(a)M$ de $C^\times$ sur l'espace S.

1. Action à l'infini. Soit v une place réelle de k et $\boldsymbol{H}$ l'algèbre des quaternions de Hamilton. On a vu que $C_v \approx \boldsymbol{H}\times\boldsymbol{H}$. Un élément de $\boldsymbol{H}$ s'écrit classiquement: $Z = x_0 + x_1 i + x_2 j + x_3 k$. Posons:

$$r_1(Z) = \begin{pmatrix} Z_1 & Z_2 \\ -\bar{Z}_2 & \bar{Z}_1 \end{pmatrix} \quad \text{avec} \quad Z_1 = x_0 + ix_1,\ Z_2 = x_2 + ix_3 \text{ dans } \boldsymbol{C}.$$

Alors r_1 est une représentation complexe de dimension 2 de $\boldsymbol{H}^\times$. Pour $l \in \boldsymbol{N}$, soit r_l la l-ième puissance symétrique de r_1. C'est une représentation irréductible de dimension $l+1$ de $\boldsymbol{H}^\times$ et toute représentation irréductible de dimension $l+1$ de $\boldsymbol{H}^\times$ est de la forme $Z \mapsto N_{\boldsymbol{H}/\boldsymbol{R}}(Z)^s r_l(Z)$, pour un $s \in \boldsymbol{C}$.

Le groupe $C_v^\times$ agit sur S_v donc aussi sur $\bar{S}_v = S_v \underset{\boldsymbol{R}}{\otimes} \boldsymbol{C}$ par $a \mapsto \mathcal{Q}_v(M)(a) = \bar{M}(a)M$.

PROPOSITION 6. *La représentation inverse $\mathcal{Q}_v(M)$ est équivalente à*

$$M \mapsto r_1(\bar{M}_1) \otimes r_1(\bar{M}_2),$$

si M est identifié à $(M_1, M_2) \in \boldsymbol{H}^\times \times \boldsymbol{H}^\times$.

Démonstration. Il est facile de voir que la représentation naturelle de $\mathrm{SO}_4(\boldsymbol{R})$ sur $\boldsymbol{C}^4$ est irréductible. Compte tenu de la proposition 4, $\mathcal{Q}_v$ est irréductible. Comme $\mathcal{Q}_v$ est une représentation inverse irréductible de $\boldsymbol{H}^\times \times \boldsymbol{H}^\times$, c'est le produit de deux représentations inverses irréductibles de $\boldsymbol{H}^\times$. Les facteurs $\boldsymbol{H}^\times$ jouant clairement le même rôle, ces deux représentations sont les mêmes, de dimension 2. Donc $\mathcal{Q}_v(M) = N_{C_v/\boldsymbol{R}}(M)^s r_1(\bar{M}_1) \otimes r_1(\bar{M}_2)$ pour un $s \in \boldsymbol{C}$ (les barres proviennent du fait que la représentation est inverse). Prenons en particulier $M = (x, x)$ avec $x \in \boldsymbol{R}^\times$. Alors par définition $\mathcal{Q}_v(M)$ est la multiplication par x^2 et le deuxième membre est la multiplication par x^{2+4s}. On en déduit $s = 0$ et la proposition. ■

Fixons un entier l pair strictement positif. On considère l'espace des polynômes p sur S_v, à coefficients complexes, homogènes de degré l, sphériques pour la forme q ([9], p. VI, 5). Cet espace est de dimension $(l+1)^2$. Le groupe $C_v^\times$ agit sur cet espace par:

$$[\tilde{R}_{l,v}(M)(p)](a) = p\left(\mathcal{Q}_v(M)a\right), \quad \text{pour } a \in S_v \text{ et } M \in C_v^\times.$$

On vérifie en effet que $\tilde{R}_{l,v}(M)(p)$ est bien sphérique pour q.

PROPOSITION 7. *La représentation $\tilde{R}_{l,v}$ de $C_v^\times$ sur l'espace des polynômes sphériques pour q, homogènes de degré l est équivalente à*

$$M = (M_1, M_2) \mapsto r_l(M_1) \otimes r_l(M_2).$$

Démonstration. D'après [15], p. 466, la représentation de $\mathrm{SO}_4(\boldsymbol{R})$ sur l'espace des polynômes sphériques homogènes de degré l est irréductible. Compte tenu de la proposition 4, on en déduit que $\tilde{R}_{l,v}$ est irréductible. On poursuit alors la démonstration de la même façon que pour la proposition 6. ■

2. Matrices de Brandt. L'entier l reste fixé dans toute la suite. Pour une place réelle v de k, on note $R_{l,v}$ la représentation matricielle complexe de dimension $(l+1)^2$ de $C_v^\times$:

$$M = (M_1, M_2) \mapsto r_l(M_1) \otimes r_l(M_2).$$

Si $M \in C$, on pose $R_l(M) = \otimes R_{l,v}(M)$ tensorisé sur toutes les places réelles de k. Soit $\mathfrak{O}_0$ l'ordre maximal de C associé au réseau L_0, et $(\mathfrak{M}_a)$

pour a allant de 1 à h, un système de représentants des classes d'idéaux d'ordre à gauche $\mathfrak{O}_0$. On note $\mathfrak{O}_a$ l'ordre à droite de $\mathfrak{M}_a$, et e_a le nombre d'éléments du quotient $\mathfrak{O}_a^\times/\mathfrak{o}_K^\times$. Soit I un idéal entier de $\mathfrak{o}_K$. On pose $\Pi(\alpha\beta, I) = \sum R_l(\overline{M})e_\beta^{-1}$, 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 que $R_l(\varepsilon M) = n_{K/\mathbf{Q}}(\varepsilon)^l R_l(M) = R_l(M)$ car l est pair).

La matrice de Brandt est alors la matrice carrée d'ordre $h(l+1)^{2[k:\mathbf{Q}]}$

$$B_l(I) = (\Pi(\alpha\beta, I)) \quad \text{pour } \alpha, \beta \text{ allant de 1 à } h.$$

3. Action de l'algèbre de Clifford en une place finie. Soit $\mathfrak{p}$ un idéal premier de $\mathfrak{o}_k$, et supposons d'abord que $\mathfrak{p}$ se décompose en $\mathfrak{P}_1\cdot\mathfrak{P}_2$ dans K. On peut alors trouver des isomorphismes rendant le diagramme suivant commutatif:

$$\begin{array}{ccc} \mathfrak{O}_{0,\mathfrak{p}} & \xrightarrow{\sim} & M_2(\mathfrak{o}_\mathfrak{p}) \times M_2(\mathfrak{o}_\mathfrak{p}) \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle j} \\ C_\mathfrak{p} & \xrightarrow{\sim} & M_2(k_\mathfrak{p}) \times M_2(k_\mathfrak{p}) \end{array}$$

où i, j, sont les injections canoniques. On identifiera $M \in C_\mathfrak{p}$ avec son image $(M_1, M_2) \in M_2(k_\mathfrak{p}) \times M_2(k_\mathfrak{p})$, la norme se transformant en l'application

$$(M_1, M_2) \mapsto (\det M_1, \det M_2) \in k_\mathfrak{p} \times k_\mathfrak{p} \approx K_\mathfrak{p}.$$

Le groupe $C_\mathfrak{p}^\times$ agit sur $S_\mathfrak{p}$ (donc aussi sur $\overline{S}_\mathfrak{p} = S_\mathfrak{p} \otimes \overline{k}_\mathfrak{p}$, où $\overline{k}_\mathfrak{p}$ est la clôture algébrique de $k_\mathfrak{p}$, et le produit tensoriel pris sur $k_\mathfrak{p}$) par $a \mapsto M(a)\overline{M}$ (on échange ici M et $\overline{M}$ pour simplifier les énoncés). On en déduit une représentation de $\mathrm{GL}_2(k_\mathfrak{p}) \times \mathrm{GL}_2(k_\mathfrak{p})$ sur $\overline{S}_\mathfrak{p}$.

Proposition 8. *Si $\mathfrak{p}$ est décomposé dans K, il existe un isomorphisme de $\overline{S}_\mathfrak{p}$ sur $\overline{k}_\mathfrak{p}^4$ tel que la représentation précédente se transforme en la représentation naturelle*

$$(M_1, M_2) \mapsto M_1 \otimes M_2.$$

Par cet isomorphisme, le $\mathfrak{o}_{k_\mathfrak{p}}$-réseau $L_{0,\mathfrak{p}}$ se transforme en le $\mathfrak{o}_{k_\mathfrak{p}}$-module engendré par la base naturelle de $\overline{k}_\mathfrak{p}^4$.

Démonstration. L'action de $C_\mathfrak{p}^\times$ sur $\overline{S}_\mathfrak{p}$ (et pas seulement sur $S_\mathfrak{p}$) est irréductible. En effet, il suffit de voir qu'un endomorphisme de $S_\mathfrak{p}$ commutant à l'action de $C_\mathfrak{p}^\times$ est forcément scalaire ([2], p. 157). Soit u un tel endomorphisme et (e_i) une base orthogonale de S. Pour $i \neq j$, notons u_{ij} l'automorphisme direct tel que $u_{ij}(e_i) = -e_i$, $u_{ij}(e_j) = -e_j$, et $u_{ij}(e_k) = e_k$ pour $k \neq i, j$. Comme u commute à u_{ij} pour tout couple (i, j) (proposition 4), un calcul rapide montre que u est diagonal dans la base (e_i). Puisque c'est vrai pour toute base orthogonale, c'est que u est

scalaire. La représentation de $\mathrm{GL}_2(k_\mathfrak{p}) \times \mathrm{GL}_2(k_\mathfrak{p})$ sur $\overline{S}_\mathfrak{p}$ étant irréductible, elle est le produit tensoriel de deux représentations irréductibles de $\mathrm{GL}_2(k_\mathfrak{p})$, qui sont bien sûr les mêmes: $M = (M_1, M_2) \mapsto R_2(M_1) \otimes R_2(M_2)$, avec R_2 de dimension 2. La représentation R_2 est clairement polynômiale (car $M \mapsto (a \mapsto M(a)\overline{M})$ l'est). De plus R_2 restreinte à $\mathrm{SL}_2(k_\mathfrak{p})$ est irréductible: sinon R_2 vaudrait 1 sur $\mathrm{SL}_2(k_\mathfrak{p})$ et serait une représentation du quotient $\mathrm{GL}_2(k_\mathfrak{p})/\mathrm{SL}_2(k_\mathfrak{p})$. Ce groupe étant abélien, R_2 serait de dimension 1, ce qui n'est pas le cas. On utilise le résultat suivant de la théorie des représentations:

Lemme 3. *A isomorphisme près, il existe une seule représentation irréductible polynômiale de degré 2 de $\mathrm{SL}_2(k_\mathfrak{p})$ sur $\overline{k}_\mathfrak{p}$. C'est la représentation naturelle.*

Sur $\mathrm{SL}_2(k_\mathfrak{p})$, on peut donc supposer que $R_2(M_1) = M_1$. Sur $k_\mathfrak{p}^\times$, soit $t \in k_\mathfrak{p}^\times$, alors $R_2(t\cdot\mathrm{Id}) \otimes R_2(\mathrm{Id})$ est isomorphe à l'action $a \mapsto M(a)\overline{M}$ avec $M = (t, 1) \in K_\mathfrak{p}$. Or pour $M \in K_\mathfrak{p}$, on sait que $M(a)\overline{M} = M M^\sigma(a) = n_{K_\mathfrak{p}/k_\mathfrak{p}}(M)a$, ici égal à $(t\cdot a)$. Donc $R_2(t\cdot\mathrm{Id}) = t\cdot\mathrm{Id}$. On a donc $R_2(M_1) = M_1$ pour $M_1 \in k_\mathfrak{p}^\times \mathrm{SL}_2(k_\mathfrak{p})$. Comme R_2 est polynômiale, on en déduit qu'elle est la représentation naturelle sur tout le groupe $\mathrm{GL}_2(k_\mathfrak{p})$, ce qui démontre la première assertion.

Le réseau $L_{0,\mathfrak{p}}$ étant stable par l'action des éléments de $\mathfrak{O}_{0,\mathfrak{p}}$, il se transforme par l'isomorphisme précédent en un $\mathfrak{o}_{k_\mathfrak{p}}$-module L_1 de rang 4, stable par l'action de l'ensemble G des matrices de $\mathrm{GL}_2(k_\mathfrak{p})^2$ à coefficients entiers. Soient (f_i) la base naturelle de $\overline{k}_\mathfrak{p}^4$ (considéré comme un espace de vecteurs colonnes), π une uniformisante de $k_\mathfrak{p}$, et $a = \sum x_i f_i$ un élément de L_1, avec $x_i \in \overline{k}_\mathfrak{p}$, et supposons $x_1 \neq 0$. Posons

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad M_\pi = \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}.$$

Soit $b = I \otimes M_\pi[M_\pi \otimes I(a) - a] - M_\pi \otimes I(a) + a$. Alors $b = (\pi-1)^2 x_1 f_1$ et $b \in L_1$. Donc $x_1 f_1 \in L_1$. Soit n le plus petit entier rationnel tel que $\pi^n x_1 f_1 \in L_1$, et modifions l'isomorphisme de $\overline{S}_\mathfrak{p}$ sur $\overline{k}_\mathfrak{p}^4$ par la multiplication par $(\pi^n x_1)^{-1}$. Alors $f_1 \in L_1$ et $\pi^{-1} f_1 \notin L$. En choisissant encore des matrices appropriées, on montre que pour $i = 1, \ldots, 4$, $f_i \in L_1$ et $\pi^{-1} f_i \notin L$. Notons L_2 le réseau sur $\mathfrak{o}_{k_\mathfrak{p}}$ de base (f_i). Alors $L_2 \subset L_1$. Il existe donc $t \in \mathfrak{o}_{k_\mathfrak{p}}$ tel que $tL_1 \subset L_2$. Si $a = \sum x_i f_i \in L_1$, on vient de voir que $x_i f_i \in L_1$. Donc $tx_i f_i \in L_2$, ce qui implique $x_i \in k_\mathfrak{p}$. Par ailleurs $\pi^{-1} f_i \notin L_1$ d'où $x_i \in \mathfrak{o}_{k_\mathfrak{p}}$ et $a \in L_2$. D'où $L_1 = L_2$, ce qui achève la démonstration. ∎

Plaçons-nous maintenant en un idéal $\mathfrak{p}$ de $\mathfrak{o}_k$ inerte dans K. On a des isomorphismes rendant le diagramme suivant commutatif:

$$\begin{array}{ccc} C_\mathfrak{p} & \xrightarrow{\sim} & M_2(K_\mathfrak{p}) \\ \downarrow & & \downarrow \\ \mathfrak{O}_{0,\mathfrak{p}} & \xrightarrow{\sim} & M_2(\mathfrak{o}_{K_\mathfrak{p}}) \end{array}$$

Le groupe $C_\mathfrak{p}^\times$ agissant toujours sur $\overline{S}_\mathfrak{p}$ par $a \mapsto M(a)\overline{M}$, on en déduit une représentation de $\mathrm{GL}_2(K_\mathfrak{p})$ sur $\overline{S}_\mathfrak{p}$.

Soit σ l'automorphisme galoisien non trivial de $K_\mathfrak{p}/k_\mathfrak{p}$. Si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K_\mathfrak{p})$, on pose $M^\sigma = \begin{pmatrix} a^\sigma & b^\sigma \\ c^\sigma & d^\sigma \end{pmatrix}$. Soit (f_i) la base naturelle de $\overline{k}_\mathfrak{p}^4$ sur $\overline{k}_\mathfrak{p}$. On définit le $\mathfrak{o}_{k_\mathfrak{p}}$-module

$$L_{1,\mathfrak{p}} = \left\{ \sum x_i f_i ;\ x_1 \text{ et } x_4 \in \mathfrak{o}_{k_\mathfrak{p}},\ x_2 \text{ et } x_3 \in \mathfrak{o}_{K_\mathfrak{p}} \text{ et } x_2 = x_3^\sigma \right\}.$$

Proposition 9. *Si* $\mathfrak{p}$ *est inerte dans* K, *il existe un isomorphisme de* $\overline{S}_\mathfrak{p}$ *sur* $\overline{k}_\mathfrak{p}^4$ *transformant la représentation précédente en la représentation* $M \mapsto M \otimes M^\sigma$. *De plus, l'image par cet isomorphisme du réseau* $L_{0,\mathfrak{p}}$ *est le* $\mathfrak{o}_{k_\mathfrak{p}}$-*module* $L_{1,\mathfrak{p}}$.

Il suffit de tensoriser la situation par $K_\mathfrak{p}$: l'algèbre $C_\mathfrak{p} \otimes K_\mathfrak{p}$ est l'algèbre de Clifford du $K_\mathfrak{p}$-espace $S_\mathfrak{p} \otimes K_\mathfrak{p}$ (les produits tensoriels sont pris sur $k_\mathfrak{p}$). Cette algèbre est décomposée. On peut trouver des isomorphismes tels que le diagramme suivant commute

$$\begin{array}{ccc} C_\mathfrak{p} \otimes K_\mathfrak{p} & \xrightarrow{\sim} & M_2(K_\mathfrak{p}) \times M_2(K_\mathfrak{p}) \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle j} \\ C_\mathfrak{p} & \xrightarrow{\sim} & M_2(K_\mathfrak{p}) \end{array}$$

où i est l'injection canonique et $j(M) = (M, M^\sigma)$. En appliquant la proposition 8 à l'espace $S_\mathfrak{p} \otimes K_\mathfrak{p}$, on obtient la première assertion. On termine la démonstration comme précédemment. ■

IV. Le théorème algébrique de relèvement

1. Enoncé du théorème. Choisissons comme en III.2 un système $(\mathfrak{M}_a)$, pour $a = 1, \ldots, h$, de représentants des classes d'idéaux de C d'ordre à gauche $\mathfrak{O}_0$. Utilisant le théorème 1, on définit des réseaux de S : $L_a = \overline{\mathfrak{M}}_a(L_0)\mathfrak{M}_a$. Posons $r = [k : \boldsymbol{Q}]$. Pour toute place réelle v de k, soit $(p_{r,v})$, pour $r = 1, \ldots, (l+1)^2$, une base de l'espace des polynômes sur S_v, sphériques pour la forme q, homogènes de degré l, pour l toujours fixé comme en III.2. Si $a \in S$, on définit les matrices colonnes :

$$p_v(a) = (p_{r,v}(a)), \quad r = 1, \ldots, (l+1)^2,$$
$$p(a) = \otimes p_v(a) \quad \text{tensorisé sur les places réelles de } k.$$

Si L est un réseau de S, n un idéal de $\mathfrak{o}_k$, on pose $m_l^0(n, L) = \sum p(a)$, sommé sur les $a \in L$ tels que $q(a)\mathfrak{o}_k = nq(L)$. Soit (h_i), pour $i = 1, \ldots, \varkappa$, un système de représentants des classes d'idéaux du corps k. Si n est un idéal de $\mathfrak{o}_k$, notons $|n| = n_{k/\boldsymbol{Q}}(n)^{-1}$. On définit les matrices colonnes à $h(l+1)^{2r}$ lignes :

$$m_l^0(n, h_i) = \left(m_l^0(n, h_i L_a)\right), \quad a = 1, \ldots, h,$$
$$m_l(n) = \sum_{i=1}^{\varkappa} |h_i|^l m_l^0(n, h_i).$$

Pour $\mathfrak{p}$ un idéal premier de $\mathfrak{o}_k$, on définit les opérateurs de Hecke :

$$T_\mathfrak{p} m_l(n) = m_l(n\mathfrak{p}) + |\mathfrak{p}|^{-(l+1)} m_l(n\mathfrak{p}^{-1}),$$
$$T_{\mathfrak{p}^2} m_l(n) = m_l(n\mathfrak{p}^2) + |\mathfrak{p}|^{-2(l+1)} m_l(n\mathfrak{p}^{-2}) - |\mathfrak{p}|^{-(l+1)} m_l(n), \quad \text{si } \mathfrak{p} \text{ divise } n,$$
$$T_{\mathfrak{p}^2} m_l(n) = m_l(n\mathfrak{p}^2) \quad \text{sinon}.$$

(On suppose que $m_l(n) = 0$ si n n'est pas entier.)

D'après la proposition 7, les représentations inverses ${}^t\tilde{R}_{l,v}(M)$ et $R_{l,r}(\overline{M})$ sont équivalentes. On suppose désormais que les bases $(p_{r,v})$ sont telles que ${}^t\tilde{R}_{l,r}(M) = R_{l,v}(\overline{M})$. D'après la définition de la représentation $\tilde{R}_{l,v}$, cela implique que pour $a \in S$ et $M \in C$, on a l'égalité :

$$\text{(A)} \qquad p\left(\overline{M}(a)M\right) = R_l(\overline{M})p(a).$$

Rappelons que pour tout idéal I de $\mathfrak{o}_K$, on a défini (III.2) des matrices de Brandt $B_l(I)$.

Théorème 2. *Soit* $\mathfrak{p}$ *un idéal premier de* $\mathfrak{o}_k$, *premier à* $\delta_{K/k}$, *et* n *un idéal de* $\mathfrak{o}_k$.

(1) *Si* $\mathfrak{p}$ *est décomposé dans* K *en* $\mathfrak{P}_1 \cdot \mathfrak{P}_2$, *on a l'égalité* :

$$\tfrac{1}{2}[B_l(\mathfrak{P}_1) + B_l(\mathfrak{P}_2)] m_l(n) = T_\mathfrak{p} m_l(n),$$

(2) *si* $\mathfrak{p}$ *est inerte dans* K, *on a l'égalité* :

$$B_l(\mathfrak{p}) m_l(n) = T_{\mathfrak{p}^2} m_l(n) + |\mathfrak{p}|^{-(l+1)} m_l(n).$$

La démonstration sera faite au § 3.

2. Réseaux primitifs de $S_\mathfrak{p}$. On se place sur $S_\mathfrak{p}$, où $\mathfrak{p}$ est premier à $\delta_{K/k}$. On pose $m = \mathfrak{p}$ si $\mathfrak{p}$ se décompose dans K, $m = \mathfrak{p}^2$ sinon. On note π une uniformisante de $k_\mathfrak{p}$, et on abandonne les indices $\mathfrak{p}$ pour alléger les notations.

Lemme 4. *Si* L *est un sous-réseau primitif de* L_0, *maximal, il existe* $M \in \mathfrak{O}_0$ *tel que* $L = M(L_0)\overline{M}$.

Démonstration. D'après le théorème 1, il existe $t \in k$ et $M \in C$ tels que $L = tM(L_0)\overline{M}$.

Si $\mathfrak{p}$ se décompose dans K, on peut supposer $t = 1$ (car $\mathfrak{p}$ est une norme). D'après la proposition 8, on peut identifier M à un couple (M_1, M_2),

avec $M_i \in \mathrm{GL}_2(k)$. Puisque $L = M_1 \otimes M_2(L_0) \subset L_0$, les termes de $M_1 \otimes M_2$ sont entiers. Mais, quitte à multiplier M par un couple (π^v, π^{-v}), on peut supposer que la matrice M_1 est entière et primitive. Alors M_2 est aussi entière. Donc $M \in \mathfrak{O}_0$.

Si $\mathfrak{p}$ est inerte dans K, on peut supposer $t = 1$ ou $t = \pi$. D'après la proposition 9, on peut identifier M à une matrice $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathrm{GL}_2(K)$. Alors $L = tM \otimes M^\sigma(L_0)$. Puisque $L \subset L_0$, les termes de $M \otimes M^\sigma$ sont dans $\pi^{-1}\mathfrak{o}_K$. Mais $n_{K/k}(a_{ij})$ sont des termes de $M \otimes M^\sigma$. Comme $\mathfrak{p}$ n'est pas une norme, cela implique que les a_{ij} sont entiers et $M \in \mathfrak{O}_0$. Puisque L est primitif, $t = 1$ d'où l'assertion. ∎

Grâce à ce lemme, on peut décrire les sous-réseaux primitifs L de L_0, maximaux de norme m. Posons $L = M(L_0)\overline{M}$.

Si $\mathfrak{p}$ se décompose dans K, on identifie M à un couple (M_1, M_2) avec M_1, M_2 entiers et $\det M_1 \det M_2 \mathfrak{o}_k = \mathfrak{p}$ (proposition 8). Le réseau $M_1 \otimes M_2(L_0)$ ne dépend que de la classe des M_i, $i = 1, 2$, dans $\mathrm{GL}_2(k)/\mathrm{GL}_2(\mathfrak{o}_k)$. Posons

$$M_\pi = \begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix}, \qquad M_u = \begin{pmatrix} \pi & u \\ 0 & 1 \end{pmatrix}$$

où u décrit un système de représentants de $\mathfrak{o}_k/\mathfrak{p}$, et $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Les sous-réseaux primitifs de L_0, maximaux de norme $\mathfrak{p}$ sont alors les $2(n_{k/\mathbf{Q}}(\mathfrak{p})+1)$ réseaux suivants:

$$(\mathrm{B}_1) \qquad L_{\pi,1} = M_\pi \otimes I(L_0), \quad L_{u,1} = M_u \otimes I(L_0), \quad L_{1,\pi} = I \otimes M_\pi(L_0), \quad L_{1,u} = I \otimes M_u(L_0).$$

Si $\mathfrak{p}$ est inerte dans K, on identifie M à un élément de $\mathrm{GL}_2(K)$ avec $\det M \mathfrak{o}_K = \mathfrak{p}\mathfrak{o}_K$ (proposition 9). Le réseau $M \otimes M^\sigma(L_0)$ ne dépend que de la classe de M dans $\mathrm{GL}_2(K)/\mathrm{GL}_2(\mathfrak{o}_K)$. Posons

$$M_\pi = \begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix} \quad \text{et} \quad M_u = \begin{pmatrix} \pi & u \\ 0 & 1 \end{pmatrix}$$

où u décrit un système de représentants de $\mathfrak{o}_K/\mathfrak{p}\mathfrak{o}_K$. Les sous-réseaux primitifs de L_0, maximaux de norme $\mathfrak{p}^2$ sont alors les $(n_{k/\mathbf{Q}}(\mathfrak{p})^2+1)$ réseaux suivants:

$$(\mathrm{B}_2) \qquad L_\pi = M_\pi \otimes M_\pi^\sigma(L_0), \quad L_u = M_u \otimes M_u^\sigma(L_0)$$

(il est immédiat que ces réseaux sont bien primitifs).

Lemme 5. *Si $a \in L_0$ est de norme divisible par m, il existe un sous-réseau primitif de L_0, maximal de norme m et contenant a.*

Démonstration. Si $a \notin \pi L_0$, on considère le réseau $L_1 = mL_0 + \mathfrak{o}a$. Il est de norme m. En effet m divise $q(L_1)$ et si $m\mathfrak{p}$ divise $q(L_1)$, alors $\mathfrak{p}^2$ divise $q(a)$ et pour tout $b \in L_0$, $m\mathfrak{p}$ divise $[b, a]m$ (où on pose $[b, a] = q(a+b) - q(a) - q(b)$). Mais alors $q(\pi^{-1}a)$ et $[b, \pi^{-1}a]$ sont entiers, donc $L_0 + \mathfrak{o}\pi^{-1}a$ est un réseau de norme $\mathfrak{o}$. Comme L_0 est maximal, cela implique $\pi^{-1}a \in L_0$ contrairement à l'hypothèse. Donc $q(L_1) = m$. Si L est un réseau contenant L_1 et de norme m, alors pour tous $b \in L$ et $c \in L_0$, m divise $q(b)$ et $[b, c]m$. Alors $q(b)$ et $[b, c]$ sont entiers, donc $L_0 + \mathfrak{o}b$ est de norme $\mathfrak{o}$ et $b \in L_0$. D'où $L \subset L_0$. Il existe alors un tel réseau L maximal, qui satisfait aux conditions du lemme.

Supposons $a \in \pi L_0$. Si $\mathfrak{p}$ se décompose dans K, L_0 est contenu dans tous les réseaux maximaux de norme $\mathfrak{p}$ et c'est terminé. Si $\mathfrak{p}$ est inerte dans K, on utilise la proposition 9 et les définitions (B_2). On pose $a = {}^t(\pi a_1, \pi a_2, \pi a_3, \pi a_4)$ avec a_1 et $a_4 \in \mathfrak{o}_k$, a_2 et $a_3 \in \mathfrak{o}_K$ et $a_2 = a_3^\sigma$. Un calcul rapide montre que:

(1) $a \in L_\pi$ équivaut à $a_4 \equiv 0 \bmod \mathfrak{p}$,

(2) $a \in L_u$ équivaut à $ua_2 + u^\sigma a_2^\sigma - uu^\sigma a_4 \equiv a_1 \bmod \mathfrak{p}$.

Si $a_4 \equiv 0 \bmod \mathfrak{p}$, alors $a \in L_\pi$ et c'est terminé. Sinon, la norme étant surjective de $\mathfrak{o}_K/\mathfrak{p}\mathfrak{o}_K$ sur $\mathfrak{o}_k/\mathfrak{p}$, il existe $v \in \mathfrak{o}_K^\times$ tel que $vv^\sigma \equiv a_4 \bmod \mathfrak{p}$. Il existe $w \in \mathfrak{o}_K$ tel que $ww^\sigma = a_2 a_2^\sigma (vv^\sigma)^{-1} - a_1 \bmod \mathfrak{p}$. Posons $u = a_2^\sigma (vv^\sigma)^{-1} + wv^{-1} \bmod \mathfrak{p}$. Alors $ua_2 + u^\sigma a_2^\sigma - uu^\sigma a_4 \equiv a_1 \bmod \mathfrak{p}$, donc $a \in L_u$. ∎

Si $a \in L_0$, on note $A(a)$ le nombre de sous-réseaux primitifs de L_0, maximaux de norme m, et contenant a. Si m ne divise pas $q(a)$, $A(a) = 0$.

Proposition 10. *Si $a \in L_0$ est de norme divisible par m, on a les égalités:*

— si $\mathfrak{p}$ se décompose dans K,

(1) *si $a \notin \pi L_0$, $A(a) = 2$,*

(2) *si $a \in \pi L_0$, $A(a) = 2(n_{k/\mathbf{Q}}(\mathfrak{p})+1)$.*

— si $\mathfrak{p}$ est inerte dans K,

(1) *si $a \notin \pi L_0$, $A(a) = 1$,*

(2) *si $a \in \pi L_0$ et $\mathfrak{p}^3$ ne divise pas $q(a)$, $A(a) = n_{k/\mathbf{Q}}(\mathfrak{p})+1$,*

(3) *si $a \in \pi L_0$, $a \notin \pi^2 L_0$ et $\mathfrak{p}^3$ divise $q(a)$, $A(a) = 1$,*

(4) *si $a \in \pi^2 L_0$, $A(a) = n_{k/\mathbf{Q}}(\mathfrak{p})^2 + 1$.*

Démonstration. Si $\mathfrak{p}$ se décompose (resp. est inerte) et $a \in \pi L_0$ (resp. $a \in \pi^2 L_0$), il est facile de voir que a est dans tous les réseaux considérés, d'où l'assertion. Si $\mathfrak{p}$ se décompose et $a \notin \pi L_0$, on utilise les définitions (B_1) et la proposition 8. On pose $a = {}^t(a_1, a_2, a_3, a_4)$ avec $a_i \in \mathfrak{o}_k$. Un calcul rapide établit les équivalences suivantes:

(1) $a \in L_{\pi,1} \Leftrightarrow a_2 \equiv a_4 \equiv 0 \bmod \mathfrak{p}$,

(2) $a \in L_{u,1} \Leftrightarrow a_1 - ua_2 \equiv a_3 - ua_4 \equiv 0 \bmod \mathfrak{p}$,

(3) $a \in L_{1,\pi} \Leftrightarrow a_3 \equiv a_4 \equiv 0 \bmod \mathfrak{p}$,

(4) $a \in L_{1,u} \Leftrightarrow a_1 - ua_3 \equiv a_2 - ua_4 \equiv 0 \bmod \mathfrak{p}$.

D'après le lemme 5, $A(a) \geqslant 1$. On peut supposer $a \in L_{\pi,1}$. Alors, comme $a \notin \pi L_0$, a n'est dans aucun réseau $L_{u,1}$. Si $a_3 \equiv 0 \bmod \mathfrak{p}$, $a \in L_{1,\pi}$

et $a \notin L_{1,u}$ pour tout u. Si $a_3 \not\equiv 0 \bmod \mathfrak{p}$, $a \notin L_{1,\pi}$ et $a \in L_{1,u}$ seulement pour $u \equiv a_1 a_3^{-1} \bmod \mathfrak{p}$. D'où la conclusion.

Si p est inerte, on utilise les définitions (B_2) et la proposition 9. D'après le lemme 5, $A(a) \geqslant 1$. On peut supposer $a \in L_\pi$. On peut poser $a = {}^t(a_1, \pi a_2, \pi a_3, \pi^2 a_4)$ avec a_1 et $a_4 \in \mathfrak{o}_k$, a_2 et $a_3 \in \mathfrak{o}_K$, et $a_2 = a_3^\sigma$. Un calcul rapide montre que $a \in L_u$ équivaut à $a_1 \equiv \pi(ua_2 + u^\sigma a_2^\sigma) \bmod \mathfrak{p}^2$. Si $a \notin \pi L_0$, alors $a_1 \not\equiv 0 \bmod \mathfrak{p}$ et $a \notin L_u$ quel que soit u, d'où l'assertion 1. Si $a \in \pi L_0$, posons $a_1 = \pi a_1'$. L'équivalence précédente devient:

$$a \in L_u \Leftrightarrow a_1' \equiv ua_2 + u^\sigma a_2^\sigma \equiv \mathrm{Tr}_{K/k}(ua_2) \bmod \mathfrak{p}.$$

L'application $u \mapsto \mathrm{Tr}_{K/k}(ua_2)$ de $\mathfrak{o}_K/\mathfrak{p}\mathfrak{o}_K$ dans $\mathfrak{o}_k/\mathfrak{p}$ est surjective, de fibres à $n_{k/\mathbf{Q}}(\mathfrak{p})$ éléments, (resp. nulle) si $a_2 \not\equiv 0 \bmod \mathfrak{p}\mathfrak{o}_K$ (resp. si $a_2 \equiv 0 \bmod \mathfrak{p}\mathfrak{o}_K$). Remarquons que la condition $a_2 \equiv 0 \bmod \mathfrak{p}\mathfrak{o}_K$ équivaut à $a = {}^t(\pi a_1', \pi^2 a_2', \pi^2 a_3', \pi^2 a_4)$ ou encore à $\pi^{-1} a \in \pi L_0 + L_\pi$. On obtient l'énoncé provisoire:

Si $a \in \pi L_0$, $a \notin \pi^2 L_0$, et $a \in L_\pi$,

(2') si $\pi^{-1} a \notin \pi L_0 + L_\pi$, $A(a) = n_{k/\mathbf{Q}}(\mathfrak{p}) + 1$,

(3') si $\pi^{-1} a \in \pi L_0 + L_\pi$, $A(a) = 1$.

Il est clair que $q(\pi L_0 + L_\pi) = \mathfrak{p}$. Si $\mathfrak{p}^3$ ne divise pas $q(a)$, alors $\mathfrak{p}$ ne divise pas $q(\pi^{-1} a)$, donc $\pi^{-1} a \notin \pi L_0 + L_\pi$ et $A(a) = n_{k/\mathbf{Q}}(\mathfrak{p}) + 1$. C'est l'assertion (2). Si $\mathfrak{p}^3$ divise $q(a)$, on a le lemme facile suivant:

Lemme 6. *Si $b \in L_0$ est de norme divisible par $\mathfrak{p}$, il existe $c \in L_0$ tel que $q(b + \pi c)$ soit divisible par $\mathfrak{p}^2$.*

Prenons $b = \pi^{-1} a$ et $c \in L_0$ tel que $\mathfrak{p}^2$ divise $q(\pi^{-1} a + \pi c)$. Alors $\pi^{-1} a + \pi c$ est dans L_π ou dans un L_u (lemme 5). Si c'est L_u, alors $\pi^{-1} a \in L_u + \pi L_0$, donc $a \in L_u$. On est dans les hypothèses de (3') avec L_u à la place de L_π, d'où $A(a) = 1$. C'est une contradiction puisque $a \in L_u$ et $a \in L_\pi$ par hypothèse. Donc $\pi^{-1} a + \pi c \in L_\pi$ et $\pi^{-1} a \in \pi L_0 + L_\pi$, d'où $A(a) = 1$. ∎

3. Démonstration du théorème 2. On pose encore $m = \mathfrak{p}$ si p se décompose dans K, $m = \mathfrak{p}^2$ si p est inerte. L'idéal n est fixé dans toute la suite. Les matrices $m_l(n)$, $m_l^0(n, h_i)$ et les matrices de Brandt apparaissent comme des matrices à h blocs. Posons

$$(B_l(\mathfrak{P}_1) + B_l(\mathfrak{P}_2))\, m_l^0(n, h_i) = (A_a(h_i)) \quad \text{où } a \text{ varie de 1 à } h,$$

ou

$$B_l(\mathfrak{p})\, m_l^0(n, h_i) = (A_a(h_i)),$$

suivant que p se décompose ou non dans K.

Posons

$$L_\beta(i, n) = \{a \in h_i L_\beta;\ q(a)\mathfrak{o}_k = nq(h_i L_\beta)\},$$

$$D_a(m) = \{(\beta, M) \in \{1, \ldots, h\} \times C^\times / \mathfrak{o}_K^\times;\ \mathfrak{M}_a^{-1}\mathfrak{M}_\beta M \text{ entier et } n_{K/k} N_{C/K}(\mathfrak{M}_a^{-1}\mathfrak{M}_\beta M) = m\}.$$

Soit f^i l'application de $D_a(m)$ dans l'ensemble des réseaux de S définie par $f^i(\beta, M) = \bar{M}(h_i L_\beta) M$. Si $b \in S$, on pose $D_a(m, b) = \{(\beta, M) \in D_a(m);\ b \in f^i(\beta, M)\}$. Les définitions impliquent:

$$A_a(h_i) = \sum_{(\beta, M)} \sum_{a} R_i(\bar{M}) e_\beta^{-1} p(a),$$

sommé sur les couples $(\beta, M) \in D_a(m)$ et les $a \in L_\beta(i, n)$. D'après la relation (Λ), on a $R_i(\bar{M}) p(a) = p(b)$ avec $b = \bar{M}(a) M$. Si $(\beta, M) \in D_a(m)$ et $a \in L_\beta(i, n)$, alors $b \in L_a(i, nm)$ (proposition 4 et théorème 1). Alors:

$$(C) \qquad A_a(h_i) = \sum_b p(b) \Big(\sum_{(\beta, M)} e_\beta^{-1} \Big),$$

sommé sur les $b \in L_a(i, nm)$ et les $(\beta, M) \in D_a(m, b)$.

Soit $f_\mathfrak{p}^i$ l'application de $D_a(m)$ dans l'ensemble des réseaux de S composée de f^i et de la localisation en p.

Lemme 7. *Si $b \in h_i L_a$, l'application $f_\mathfrak{p}^i$, restreinte à $D_a(m, b)$, est une surjection sur l'ensemble des sous-réseaux primitifs de $(h_i L_a)_\mathfrak{p}$, maximaux de norme $mq(h_i L_{a,\mathfrak{p}})$, qui contiennent b. La fibre de cette application au point $f_\mathfrak{p}^i(\beta, M)$ a e_β éléments.*

Démonstration. Vérifions d'abord que l'image de $f_\mathfrak{p}^i$ est contenue dans l'ensemble de réseaux indiqué. Localement les idéaux sont principaux, donc il existe $M_{a\beta} \in C_\mathfrak{p}^\times$ tel que $\mathfrak{M}_{\beta,\mathfrak{p}} = \mathfrak{M}_{a,\mathfrak{p}} M_{a\beta}$. Si $(\beta, M) \in D_a(m)$, alors $f_\mathfrak{p}^i(\beta, M) = \bar{M}'(h_i L_{a,\mathfrak{p}}) M'$, avec $M' = M_{a\beta} M$. Les conditions sur M entraînent que $M' \in \mathfrak{O}_{a,\mathfrak{p}}$ et $n_{K_\mathfrak{p}/k_\mathfrak{p}} N_{C_\mathfrak{p}/K_\mathfrak{p}}(M')\mathfrak{o}_\mathfrak{p} = m\mathfrak{o}_\mathfrak{p}$. D'après IV.2, $f_\mathfrak{p}^i(\beta, M)$ est bien un sous-réseau primitif de $h_i L_{a,\mathfrak{p}}$ de la norme voulue.

Réciproquement, soit $L_\mathfrak{p}$ un tel sous-réseau contenant b. Il existe $M_\mathfrak{p} \in \mathfrak{O}_{a,\mathfrak{p}}$ tel que $L_\mathfrak{p} = \bar{M}_\mathfrak{p}(h_i L_{a,\mathfrak{p}}) M_\mathfrak{p}$ (lemme 4). On définit l'idéal

$$\mathfrak{M} = \mathfrak{M}_{a,\mathfrak{p}} M_\mathfrak{p} \cap \bigcap_{\mathfrak{q} \neq \mathfrak{p}} \mathfrak{M}_{a,\mathfrak{q}}.$$

Il existe β et $M \in C^\times$ tel que $\mathfrak{M} = \mathfrak{M}_\beta M$. Alors le couple (β, M) appartient à $D_a(m)$ et $f_\mathfrak{p}^i(\beta, M) = L_\mathfrak{p}$. De plus $b \in f^i(\beta, M)$ car $f^i(\beta, M) = L_\mathfrak{p} \cap \bigcap_{\mathfrak{q} \neq \mathfrak{p}} h_i L_{a,\mathfrak{q}}$.

Enfin si (β_1, M_1) et (β_2, M_2) sont dans $D_a(m, b)$, on a $f_\mathfrak{q}^i(\beta_j, M_j) = h_i L_{a,\mathfrak{q}}$ pour $j = 1, 2$ et pour tout $\mathfrak{q} \neq \mathfrak{p}$. Si $f_\mathfrak{p}^i(\beta_1, M_1) = f_\mathfrak{p}^i(\beta_2, M_2)$, alors $f^i(\beta_1, M_1) = f^i(\beta_2, M_2)$. Il existe donc un idéal I de K tel que $\mathfrak{M}_{\beta_1} M_1 = I\mathfrak{M}_{\beta_2} M_2$ (théorème 1). Alors $N_{C/K}(\mathfrak{M}_a^{-1}\mathfrak{M}_{\beta_1} M_1) = I^2 N_{C/K}(\mathfrak{M}_a^{-1}\mathfrak{M}_{\beta_2} M_2)$. Cela entraîne facilement que $I = \mathfrak{o}_K$. D'où $\mathfrak{M}_{\beta_1} M_1 = \mathfrak{M}_{\beta_2} M_2$. Donc $\beta_1 = \beta_2$ et il existe $\mu \in \mathfrak{O}_\beta^\times$ tel que $M_1 = \mu M_2$. ∎

Les idéaux étant localement principaux, on peut se ramener au cas où $h_i L_{a,\mathfrak{p}} = L_{0,\mathfrak{p}}$. Le lemme 7 et la relation (C) impliquent: $A_a(h_i) = \sum_b p(b) A(b)$, sommé sur les $b \in L_a(i, nm)$, où $A(b)$ est donné par la proposition 10.

Si p se décompose dans K, on obtient

$$A_a(h_i) = 2\sum p(b) + 2(|\mathfrak{p}|^{-1}+1)\sum p(b),$$

la $1^{\text{ère}}$ somme étant prise sur les éléments p-primitifs de $L_a(i, n\mathfrak{p})$, la $2^{\text{ème}}$ sur les imprimitifs.

Ou encore $A_a(h_i) = 2\sum p(b) + 2|\mathfrak{p}|^{-1}\sum p(b)$, la $1^{\text{ère}}$ somme prise sur tous les $b \in L_a(i, n\mathfrak{p})$, la $2^{\text{ème}}$ sur les éléments imprimitifs de $L_a(i, n\mathfrak{p})$. Ces derniers sont les $b \in \mathfrak{p}h_iL_a$ tels que $q(b)\mathfrak{o}_k = n\mathfrak{p}q(h_iL_a) = n\mathfrak{p}^{-1}q(\mathfrak{p}h_iL_a)$. D'où

$$A_a(h_i) = 2m_l^0(n\mathfrak{p}, h_iL_a) + 2|\mathfrak{p}|^{-1}m_l^0(n\mathfrak{p}^{-1}, \mathfrak{p}h_iL_a).$$

C'est parce qu'on ne sait pas comparer h_iL_a et $\mathfrak{p}h_iL_a$ quand p n'est pas principal qu'on introduit $m_l(n) = \sum_{i=1}^{\varkappa} |h_i|^l m_l^0(n, h_i)$. Posons

$$[B_l(\mathfrak{P}_1) + B_l(\mathfrak{P}_2)]m_l(n) = (A_a), \quad a = 1, \ldots, h.$$

Alors

$$A_a = 2\sum_i |h_i|^l m_l^0(n\mathfrak{p}, h_iL_a) + 2|\mathfrak{p}|^{-1}\sum_i |h_i|^l m_l^0(n\mathfrak{p}^{-1}, \mathfrak{p}h_iL_a).$$

Soit $i \in \{1, \ldots, \varkappa\}$. Il existe $t \in k$ et j tel que $\mathfrak{p}h_i = th_j$. L'homogénéité des polynômes sphériques entraîne

$$m_l^0(n\mathfrak{p}^{-1}, \mathfrak{p}h_iL_a) = n_{k/\mathbf{Q}}(t)^l m_l^0(n\mathfrak{p}^{-1}, h_jL_a) = |h_j|^l|\mathfrak{p}h_i|^{-l}m_l^0(n\mathfrak{p}^{-1}, h_jL_a).$$

L'application $h_i \mapsto h_j$ étant bijective, on obtient finalement:

$$[B_l(\mathfrak{P}_1) + B_l(\mathfrak{P}_2)]m_l(n) = 2m_l(n\mathfrak{p}) + 2|\mathfrak{p}|^{-(l+1)}m_l(n\mathfrak{p}^{-1}).$$

C'est l'assertion du théorème.

Si p est inerte dans K, on a de la même façon:

(1) si p ne divise pas n,

$$A_a(h_i) = \sum p(b) + (|\mathfrak{p}|^{-1}+1)\sum p(b),$$

la $1^{\text{ère}}$ somme étant prise sur les éléments p-primitifs de $L_a(i, n\mathfrak{p}^2)$, la $2^{\text{ème}}$ sur les imprimitifs.

(2) si p divise n,

$$A_a(h_i) = \sum p(b) + (|\mathfrak{p}|^{-2}+1)\sum p(b),$$

la $1^{\text{ère}}$ somme prise sur les $b \in L_a(i, n\mathfrak{p}^2)$ tels que $b \notin \mathfrak{p}^2h_iL_a$, la $2^{\text{ème}}$ sur les $b \in L_a(i, n\mathfrak{p}^2)$ tels que $b \in \mathfrak{p}^2h_iL_a$.

On termine la démonstration comme dans le cas décomposé.

Remarque. L'utilisation qu'on a faite des représentations locales de l'algèbre de Clifford revient essentiellement à reformuler des résultats de Eichler sur la structure locale des réseaux maximaux [4].

V. Séries thêta sur K

Dans ce paragraphe, on restera uniquement sur le corps K. On renvoie à [16] pour la théorie des formes automorphes.

1. Rappels et notations. On note $\boldsymbol{A}$ l'anneau des adèles de K, $\boldsymbol{I}$ le groupe des idèles, $\mathscr{I}_K$ le groupe des idéaux, I_K le groupe des classes d'idéaux. Si $t \in \boldsymbol{I}$ on note $\mathrm{div}(t)$ l'idéal naturellement associé à t. Soient d l'idèle différentielle de K ([16], p. 11), ψ l'unique caractère de $\boldsymbol{A}/K$ tel qu'en toute place v réelle de K on ait $\psi_v(x) = e^{2\pi ix}$ (on inverse ici la convention de [16]). On pose

$$G = \mathrm{GL}(2), \qquad B = \left\{\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(2)\right\}.$$

Si Φ est une fonction sur G, on notera $\Phi(x, y)$ sa restriction à B. Notons enfin (v_i), $i = 1, \ldots, r'$, les valuations réelles de K, et si $x \in \boldsymbol{A}$, x_i sa composante dans K_{v_i}.

On considère les caractères η non ramifiés de $\boldsymbol{I}$ (i.e. qui se factorisent par l'application naturelle $\boldsymbol{I} \to I_K$). Si Φ est une forme automorphe sur $G_{\boldsymbol{A}}$, de poids $n \in \boldsymbol{N}^*$, de caractère η, parabolique, il existe une fonction $c: \mathscr{I}_K \to \boldsymbol{C}$, telle que $c(J) = 0$ si J n'est pas entier, et telle que ([16], p. 20 et 120):

(D) pour $x \in \boldsymbol{I}$, $y \in \boldsymbol{A}$,

$$\Phi(x, y) = \sum_{\xi} c(\mathrm{div}(\xi dx))\Big(\prod_{i=1}^{r'} |\xi x|_i^{n/2}\exp(-2\pi\xi_i x_i)\Big)\psi(\xi y),$$

sommé sur les $\xi \in K^\times$ tels que ξx soit totalement positif.

Réciproquement, soit $\Phi(x, y)$ une fonction définie sur $B_{\boldsymbol{A}}$ par l'égalité (D), qu'on suppose suffisamment convergente. On dit qu'un couple (x, y) est écrit sous forme réduite si $(x, y) = (tf, te)$, où $t_v = (x_v^2 + y_v^2)^{1/2}$ si v est réelle, et $\sup(|f|_v, |e|_v) = 1$ si v est finie. En une place réelle v_j, on définit θ_j par $\cos\theta_j = e_{v_j}$, $\sin\theta_j = -f_{v_j}$.

Proposition 11 ([16], p. 28). *La fonction $\Phi(x, y)$ se prolonge à $G_{\boldsymbol{A}}$ en une forme automorphe de poids n, de caractère η, parabolique, si pour tout couple réduit (tf, te) et pour toute adèle e' telle que $e'_v = -e_v$ si v est réelle, et $|1 + ee'|_v \leqslant |f|_v$ si v est finie, on a l'égalité:*

$$\Phi(tf, te) = \Phi(t^{-1}f, t^{-1}e')\Big(\prod_{j=1}^{r'} \exp(in\theta_j)\Big)\eta(t).$$

2. Séries thêta. Soient $\mathfrak{O}$ un ordre maximal de C, $\mathfrak{M}$ un $\mathfrak{O}$-idéal à gauche, l un entier pair strictement positif, et pour tout $i = 1, \ldots, r'$, P_i un polynôme sphérique sur l'algèbre C_{v_i}, homogène de degré l. Pour un

idéal J de $\mathfrak{o}_K$, on pose

$$c(J) = |J|^{(l+2)/2} \sum_{M} \Big(\prod_{i=1}^{r'} P_i(M) \Big),$$

sommé sur les $M \in \mathfrak{M}$ tels que $N_{C/K}(M)\mathfrak{o}_K = JN_{C/K}(\mathfrak{M})$, et où on ne prend qu'un élément dans un ensemble $\{\varepsilon M; \varepsilon \in \mathfrak{o}_K^\times\}$. Soit $n = l+2$. Par la formule (D), on associe à cette fonction c une fonction $\Phi^0_{\mathfrak{M}}(x, y)$ sur $B_{\boldsymbol{A}}$.

PROPOSITION 12. (a) *Si (tf, te) est un couple réduit et e' une adèle comme dans l'énoncé de la proposition* 11, *on a l'égalité*

$$|N_{C/K}(\mathfrak{M})|^{l/2} \Phi^0_{\mathfrak{M}}(tf, te) = |N_{C/K}(\mathfrak{M}\mathrm{div}\, t)|^{l/2} \Phi^0_{\mathfrak{M}\,\mathrm{div}\, t}(t^{-1}f, t^{-1}e') \prod_{j=1}^{r'} e^{i(l+2)\theta_j};$$

(b) *pour tout couple (x, y) et tout $\xi \in K^\times$, on a l'égalité*:

$$|N_{C/K}(\xi\mathfrak{M})|^{l/2} \Phi^0_{\xi\mathfrak{M}}(x, y) = |N_{C/K}(\mathfrak{M})|^{l/2} \Phi^0_{\mathfrak{M}}(x, y).$$

La démonstration sera donnée au § 3.

Ici encore, on est gêné par le fait qu'on ne peut pas comparer les séries $\Phi^0_{\mathfrak{M}}$ et $\Phi^0_{\mathfrak{M}\,\mathrm{div}\, t}$ quand $\mathrm{div}\, t$ n'est pas principal. Soit (I_k), $k = 1, \ldots, \varkappa'$ un système de représentants du groupe des classes d'idéaux de K, et η un caractère non ramifié de $\boldsymbol{I}$. Posons:

$$\Phi_{\mathfrak{M},\eta}(x, y) = \sum_{k=1}^{\varkappa'} |N_{C/K}(\mathfrak{M}I_k)|^{l/2} \eta^{-1}(I_k) \Phi^0_{\mathfrak{M}I_k}(x, y).$$

PROPOSITION 13. *La fonction $\Phi_{\mathfrak{M},\eta}(x, y)$ se prolonge en une forme automorphe parabolique sur $G_{\boldsymbol{A}}$, de poids $l+2$ et de caractère η.*

Cela résulte des propositions 11 et 12, en remarquant que l'application $J \mapsto J\,\mathrm{div}\, t$, de $\mathscr{I}_K$ dans lui-même définit une bijection sur le groupe des classes d'idéaux I_K. ■

3. Démonstration de la proposition 12. On identifie C à K^4, considéré comme un ensemble de vecteurs colonnes, on note A la matrice de la forme $N_{C/K}$ (notée N) dans la base canonique de K^4. Si $m \in K^4$, on pose $N^*(m) = \frac{1}{2}{}^t m A^{-1} m$. On note ψ_v, $|\cdot|_v$ (resp. ψ_f, $|\cdot|_f$, resp. ψ_∞, $|\cdot|_\infty$) la restriction de ψ et la valuation en une place v (resp. leur produit aux places finies, resp. leur produit aux places réelles). Si $m \in K^4$, on pose $P_\infty(m) = \prod_{j=1}^{r'} P_j(m)$. Si (z_j), $j = 1, \ldots, r'$, sont des nombres complexes, on pose $z_\infty = \prod_j z_j$, $e_\infty(z) = \prod_j \exp(z_j)$. Soit χ_v la fonction caractéristique de $\mathfrak{M}_v$.

Donnons-nous des complexes z_j, $\mathrm{Im}(z_j) > 0$, pour $j = 1, \ldots, r'$, et $w \in \boldsymbol{A}$. On définit $w_1 \in \boldsymbol{A}$: $w_{1,v}$ est un générateur de $d^{-1}N(\mathfrak{M}_v)^{-1}$ si

$w_v \in d^{-1}N(\mathfrak{M}_v)^{-1}$, pour v finie, et $w_{1,v} = w_v$ aux autres places. Soit $m \in K_v^4$.

Si $v = v_j$ est réelle, soit

$$f_v(m) = P_j(m) \exp\big(2\pi i z_j N(m)\big),$$

si v est finie, soit

$$f_v(m) = \psi_v\big(N(m)w\big)\chi_v(m).$$

Pour $\mu \in K_v^4$, on pose

$$g_v(\mu) = \int_{K_v^4} f_v(m)\psi_v(-{}^t\mu m)\, d_v m,$$

où $d_v m$ est la mesure de Haar convenablement normalisée ([13], p. 319).

LEMME 8. (a) *Si $v = v_j$ est réelle, on a l'égalité*

$$g_v(\mu) = -|\det A|_v^{-1/2} z_j^{-(l+2)} P_j(A^{-1}\mu) \exp\big(-2\pi i N^*(\mu) z_j^{-1}\big).$$

(b) *Si v est finie, on a les égalités*

$$g_v(\mu) = 0 \quad \text{si} \quad A^{-1}\mu \notin w_1\mathfrak{M}_v,$$

$$g_v(\mu) = |w_1|_v^{-2} |\det A|_v^{-1/2} \psi_v\big(-N^*(\mu)w_1^{-1}\big), \quad \text{si} \quad A^{-1}\mu \in w_1\mathfrak{M}_v.$$

Démonstration. En une place réelle, le calcul est classique ([9], p. VI 14). En une place finie, il existe un isomorphisme S de K_v^4 dans lui-même tel que $S\mathfrak{M}_v = \mathfrak{o}_v^4$ et si $Sm = m'$, $N(m) = n(m_1'm_4' - m_2'm_3')$, où n est un générateur de $N(\mathfrak{M}_v)$. Alors

$$g_v(\mu) = |\det S|_v^{-1} \int_{\mathfrak{o}_v^4} \psi_v[nw(m_1m_4 - m_2m_3) - {}^t\mu S^{-1} m]\, d_v m.$$

Cette intégrale est facilement calculable et conduit au résultat ci-dessus. ■

Posons

$$F(\mathfrak{M}, (z_j), w) = \sum_{M \in \mathfrak{M}} P_\infty(M) e_\infty\big(2\pi i z N(M)\big) \psi_f\big(N(M)w\big).$$

LEMME 9. *Pour tout ensemble (z_j) d'éléments du demi-plan de Poincaré, et $w \in \boldsymbol{A}$, on a*

$$F(\mathfrak{M}, (z_j), w) = z_\infty^{-(l+2)} |w_1|_f^{-2} F\big(w_1\mathfrak{M}, (-z_j^{-1}), -w_1^{-1}\big).$$

Démonstration. Si $m \in \boldsymbol{A}^4$, posons $f(m) = \prod_v f_v(m)$ sur toutes les places de K, et $G(m) = \sum f(M+m)$, sommé sur les $M \in K^4$. Alors $F(\mathfrak{M}, (z_j), w) = G(0)$. Comme G est continue périodique, de période K^4, et intégrable sur $\boldsymbol{A}^4/K^4$, elle est égale à sa série de Fourier ([13], p. 332):

$$G(m) = \sum_{\mu \in K^4} g(\mu)\psi({}^t\mu m), \quad \text{avec} \quad g(\mu) = \int_{\boldsymbol{A}^4/K^4} G(m)\psi(-{}^t\mu m)dm.$$

Alors

$$g(\mu) = \int_{A^4} f(m)\psi(-{}^t\mu m)dm = \prod_v \int_{K_v^4} f_v(m)\psi_v(-{}^t\mu m)d_v m.$$

D'où (lemme 8) $g(\mu) = 0$ si $A^{-1}\mu \notin w_1\mathfrak{M}$,

$$g(\mu) = |w_1|_f^{-2}\Big(\prod_v |\det A|_v\Big)^{-1/2} z_\infty^{-(l+2)} P_\infty(A^{-1}\mu)\, e_\infty\big(-2\pi i N^*(\mu)z^{-1}\big) \times \\ \times \psi_f\big(-N^*(\mu)w_1^{-1}\big),$$

si $A^{-1}\mu \in w_1\mathfrak{M}$ (les signes $-$ disparaissent car r' est pair).

Comme $\det A \in K$, $\prod_v |\det A|_v = 1$. En reportant cette valeur dans l'expression de $G(m)$, en sommant sur $\mu' = A^{-1}\mu$, et en posant $m = 0$, on obtient le lemme. ■

Soient $E = \mathfrak{o}_K^\times$, E^+ le groupe des unités totalement positives, et (ε) un système de représentants du quotient E^+/E^2. Si $x \in \boldsymbol{I}$, on note $x \gg 0$ si x est totalement positif. Soit $x \in \boldsymbol{I}$. S'il existe $\xi \in K$ tel que $\xi x \gg 0$ et $N(\mathfrak{M})\mathrm{div}(dx) = \xi\mathfrak{o}_K$, on choisira un tel élément, noté $\xi(x)$.

Lemme 10. *Soient $x \in \boldsymbol{I}$, $y \in \boldsymbol{A}$, alors*

(1) *si $\xi(x)$ n'existe pas,*

$$\Phi^0_{\mathfrak{M}}(x, y) = 0,$$

(2) *si $\xi(x)$ existe,*

$$\Phi^0_{\mathfrak{M}}(x, y) = \tfrac{1}{2}|d|_f^{(l+2)/2}|x|^{(l+2)/2}\sum_\varepsilon F\big(\mathfrak{M}, \big((y+ix)/\xi(x)\varepsilon\big), y/\xi(x)\varepsilon\big).$$

Démonstration. La formule (D) est sommée sur les $\xi \in K^\times$ tels que $\xi x \gg 0$. On a $c\big(\mathrm{div}(\xi dx)\big) = |\xi dx|_f^{(l+2)/2}\sum_M P_\infty(M)$, sommé sur les $M \in \mathfrak{M}$, à une unité près, tels que $N(M)\mathfrak{o}_K = \mathrm{div}(\xi dx)N(\mathfrak{M})$. Comme $N(M) \gg 0$, on en déduit que $c\big(\mathrm{div}(\xi dx)\big) = 0$ pour tout ξ si $\xi(x)$ n'existe pas. Si $\xi(x)$ existe, on somme sur les $\xi \in K^\times$, les $M \in \mathfrak{M}$, à une unité près, tels que $N(M) = \xi\xi(x)\mu$, avec un $\mu \in E^+$, ou encore sur ε, sur ξ, et sur $M \in \mathfrak{M}$ au signe près, tels que $N(M) = \xi\xi(x)\varepsilon$. Remplaçons ξ par $N(M)\xi(x)^{-1}\varepsilon^{-1}$ dans la formule (D). On obtient:

$$\Phi^0_{\mathfrak{M}}(x, y) = \tfrac{1}{2}\sum_\varepsilon\sum_{M\in\mathfrak{M}} |dx|_f^{(l+2)/2}|x|_\infty^{l+2}P_\infty(M)\, e_\infty\big(-2\pi x N(M)\xi(x)^{-1}\varepsilon^{-1}\big) \times \\ \times\psi\big(N(M)y\,\xi(x)^{-1}\varepsilon^{-1}\big)$$

(le $\frac{1}{2}$ provient de la sommation sur M au signe près). Développons le caractère ψ aux places réelles, on obtient le lemme. ■

Démontrons maintenant la proposition 12. Le (b) est immédiat. Soit $(x, y) = (tf, te)$, $(x', y') = (t^{-1}f, t^{-1}e')$. Si $\xi(x)$ n'existe pas, $\xi'(x')$ (rapporté à l'idéal $\mathfrak{M}\,\mathrm{div}\,t$) n'existe pas non plus et les deux membres de l'égalité (a) sont nuls. Si $\xi(x)$ existe, on peut poser $\xi'(x') = \xi(x)$. On développe $\Phi^0_{\mathfrak{M}}(x, y)$ en utilisant le lemme 10. Fixons ε et soit $z_j = \big((y+ix)/\xi(x)\varepsilon\big)_j$, $w = y/\xi(x)\varepsilon$.

En une place réelle v_j, on a:

$$z^{-1} = \xi(x)\varepsilon t^{-1}(e+if)^{-1} = -\xi(x)\varepsilon(e'+if)/t = -\xi(x)^2\varepsilon(y'+ix')/\xi'(x').$$

D'autre part, $z_j^{-1} = \big(\xi(x)\varepsilon/t\big)\exp(i\theta_j)$.

En une place finie v, la condition $w \notin d^{-1}N(\mathfrak{M})^{-1}$ équivaut à $y \notin \xi(x)d^{-1}N(\mathfrak{M})^{-1} = \mathrm{div}\,x$, ou encore $e \notin f\mathfrak{o}_v$, c'est-à-dire $f \notin \mathfrak{o}_v^\times$ (puisque $\sup(|e|_v, |f|_v) = 1$). Si $f \notin \mathfrak{o}_v^\times$ alors $w_1 = y/\xi(x)\varepsilon$, d'où $|w_1|_v = |t\xi(x)^{-1}|_v$. Si $f \in \mathfrak{o}_v^\times$, w_1 engendre $d^{-1}N(\mathfrak{M})^{-1} = \mathrm{div}\big(x\,\xi(x)^{-1}\big)$, d'où encore $|w_1|_v = |t\,\xi(x)^{-1}|_v$. Donc $w_1\mathfrak{M} = \mathfrak{M}\mathrm{div}\big(t\,\xi(x)^{-1}\big)$.

Posons $w' = y'\varepsilon/\xi'(x')$. Pour $M \in w_1\mathfrak{M}$, on a $\psi_f\big(-N(M)w_1^{-1}\big) = \psi_f\big(N(M)\,\xi(x)^2w'\big)$. En effet, en une place finie v, si $f \in \mathfrak{o}_v^\times$, les deux membres sont égaux à 1. Si $f \notin \mathfrak{o}_v^\times$, il suffit de voir que $N(M)\big(\xi(x)^2w' + w_1^{-1}\big) \in d^{-1}\mathfrak{o}_v$. Mais

$$N(M)\big(\xi(x)^2w' + w_1^{-1}\big) = N(M)\varepsilon\xi(x)(y' + y^{-1}) = N(M)\varepsilon\xi(x)t^{-1}e^{-1}(1+ee').$$

En utilisant l'hypothèse $|1+ee'|_v \leqslant |f|_v$, on obtient le résultat.

Utilisons le lemme 9 et ces résultats. On obtient:

$$\Phi^0_{\mathfrak{M}}(x, y) = \tfrac{1}{2}|d|_f^{(l+2)/2}Ce_\infty\big(i(l+2)\theta\big) \times \\ \times\sum_\varepsilon F\big(\mathfrak{M}\mathrm{div}\,t,\ (\varepsilon(y'+ix')/\xi'(x'))_f,\ y'\varepsilon/\xi'(x')\big),$$

avec

$$C = |x|^{(l+2)/2}|\xi(x)t^{-1}|_f^2\big(\xi(x)\varepsilon t^{-1}\big)_\infty^{l+2}\,\xi(x)_\infty^{-1}.$$

On calcule facilement C. En utilisant à nouveau le lemme 10, on obtient la proposition. ■

4. Matrices de Brandt réduites. On va modifier les matrices de Brandt pour tenir compte de la proposition 13. Soit $\mathfrak{O}_0$ l'ordre maximal de C associé au réseau L_0, et $\mathfrak{O}_\alpha$, pour $\alpha = 1, \ldots, h'$, un système de représentants des classes d'ordres maximaux, pour l'équivalence par automorphisme intérieur de C. Soit $\mathfrak{M}_\alpha$ un idéal d'ordres à gauche $\mathfrak{O}_0$ et à droite $\mathfrak{O}_\alpha$, et toujours (I_k), $k = 1, \ldots, \varkappa'$ un système de représentants des classes d'idéaux de K. Notons $\varkappa'_\alpha$ le cardinal du sous-groupe du groupe des classes d'idéaux de K formé des idéaux I tels que $\mathfrak{O}_\alpha I$ soit principal. Soit $\mathfrak{M}$ un idéal de C d'ordre à droite $\mathfrak{O}_\beta$, et I un idéal de $\mathfrak{o}_K$. On pose $\Pi^0(\mathfrak{M}, I) = \sum R_l(\overline{M})e_\beta^{-1}$, sommé sur les $M \in \mathfrak{M}$ tels que $N_{C/K}(M)\mathfrak{o}_K = IN_{C/K}(\mathfrak{M})$, à une unité de $\mathfrak{o}_K$ près,

$$\Pi_\eta(\alpha, \beta, I) = \frac{1}{\varkappa'_\beta}\sum_{k=1}^{\varkappa'} |I_k|^l\eta^{-1}(I_k)\Pi^0(\mathfrak{M}_\beta^{-1}\mathfrak{M}_\alpha I_k, I).$$

La matrice de Brandt réduite de caractère η est alors:

$$B_l(\eta, I) = (\Pi_\eta(\alpha, \beta, I)), \quad \alpha, \beta = 1, \ldots, h'.$$

PROPOSITION 14. *Les matrices de Brandt réduites vérifient les propriétés de multiplicativité suivantes:*

(a) $B_l(\eta, I)B_l(\eta, J) = B_l(\eta, IJ)$ *pour* I *et* J *premiers entre eux,*

(b) $B_l(\eta, \mathfrak{P}^n)B_l(\eta, \mathfrak{P}^m) = \sum_t \eta(\mathfrak{P})^t |\mathfrak{P}|^{-(l+1)t} B_l(\eta, \mathfrak{P}^{m+n-2t})$, *sommé de* $t = 0$ *à* $t = \min(m, n)$, *si* $\mathfrak{P}$ *est premier.*

En particulier, pour η fixé, elles commutent.

PROPOSITION 15. *Les matrices de Brandt réduites sont diagonalisables.*

COROLLAIRE. *Pour* η *fixé, les matrices de Brandt réduites* $B_l(\eta, I)$ *diagonalisent dans une même base.*

Les démonstrations sont des transcriptions dans le cas où K n'est pas de nombre de classes 1 des démonstrations de [5]. ∎

Si I est un idéal de $\mathfrak{o}_K$, posons $c_\eta(I) = |I|^{(l+2)/2} B_l(\eta, I)$. La formule (D) associe à cette fonction c_η une fonction Φ_η sur B_A (à valeurs dans l'ensemble des matrices carrées d'ordre $h'(l+1)^{r'}$).

PROPOSITION 16. *Les termes de la fonction matricielle* Φ_η *se prolongent en des formes automorphes sur* G_A, *paraboliques de poids* $l+2$ *et de caractère* η.

En effet les coefficients de $R_l(M)$ sont des polynômes sphériques ([5], p. 30), et la modification des matrices de Brandt permet d'appliquer la proposition 13. ∎

5. Opérateurs de Hecke. Soit Φ une forme automorphe sur G_A de poids $l+2$ et de caractère η, c sa fonction associée par (D). Si $\mathfrak{P}$ est un idéal premier de $\mathfrak{o}_K$, soit $T_\mathfrak{P}$ l'opérateur de Hecke associé ([16], p. 41), et $T_\mathfrak{P} c$ la fonction associée à $T_\mathfrak{P}\Phi$. On a:

$$T_\mathfrak{P} c(I) = |\mathfrak{P}|^{-(l+2)/2} c(I\mathfrak{P}) + |\mathfrak{P}|^{-l/2} \eta(\mathfrak{P}) c(I\mathfrak{P}^{-1}) \quad ([16], \text{p. } 42).$$

PROPOSITION 17. *On a l'égalité* $T_\mathfrak{P}\Phi_\eta = B_l(\eta, \mathfrak{P})\Phi_\eta$.

Cela résulte des définitions et de la proposition 14.

6. L'espace des formes automorphes sur K. Notons $\mathscr{A}_0(K, l+2, \eta)$ l'espace des formes automorphes paraboliques sur K, de caractère η non ramifié, de poids $l+2$, et $\mathscr{A}_0(K, l+2) = \oplus \mathscr{A}_0(K, l+2, \eta)$ sur tous les caractères non ramifiés. La définition de $\Phi_{\mathfrak{M},\eta}$ à partir de $\Phi^0_\mathfrak{M}$ (V.2) revient à calculer la composante sur $\mathscr{A}_0(K, l+2, \eta)$ d'un élément de $\mathscr{A}_0(K, l+2)$. Une série thêta classique $\Phi^0_\mathfrak{M}$ est donc un élément de $\mathscr{A}_0(K, l+2)$. Soit $c(I) = |I|^{(l+2)/2} B_l(I)$ et $\Phi(x, y)$ la fonction matricielle sur B_A associée par (D) à la fonction c. Les termes de $\Phi(x, y)$ se prolongent à G_A en des éléments de $\mathscr{A}_0(K, l+2)$. Eichler a calculé la trace des matrices de Brandt [6]. Shimizu a calculé celle des opérateurs de Hecke [12], et on vérifie qu'il l'a calculée dans $\mathscr{A}_0(K, l+2)$. Ces deux traces sont les mêmes [14].

THÉORÈME 3. *Sur un corps de nombres totalement réel* K *de degré pair sur* $\mathbf{Q}$, *l'espace* $\mathscr{A}_0(K, l+2)$ *est engendré par les séries thêta coefficients de* Φ.

Démonstration. Notons $\mathrm{Tr}(I)$ la trace de l'opérateur de Hecke T_I sur $\mathscr{A}_0(K, l+2)$, et soit $(\Phi_{i,\eta})$, $i = 1, \ldots, d_\eta$, une base de $\mathscr{A}_0(K, l+2, \eta)$ avec $\Phi_{i,\eta}$ propre pour tous les opérateurs de Hecke, et normalisée. Soit $\Phi' = \sum_\eta \sum_i \Phi_{i,\eta}$. La fonction c' associée à Φ' est alors $c'(I) = |I|^{(l+2)/2}\mathrm{Tr}(I)$. D'après les résultats de Eichler et Shimizu, on a donc $\Phi' = \mathrm{Tr}(\Phi)$. Donc Φ' est dans l'espace engendré par les termes de Φ. Alors ses composantes $\sum_i \Phi_{i,\eta}$ sont dans les espaces engendrés par les termes de Φ_η. Or, comme dans le cas à une variable, $\sum_i \Phi_{i,\eta}$ et ses transformés par les opérateurs de Hecke engendrent $\mathscr{A}_0(K, l+2, \eta)$. L'espace des termes de Φ_η étant stable par les opérateurs de Hecke, cet espace coïncide avec $\mathscr{A}_0(K, l+2, \eta)$. Comme un terme de Φ_η est combinaison linéaire de termes de Φ, on en déduit le théorème. ∎

VI. Le relèvement

On suppose $k = \mathbf{Q}$. Les hypothèses se traduisent par le choix d'un nombre Δ_1 sans carrés, positif. On pose $\Delta = \Delta_1$ si $\Delta_1 \equiv 1 \bmod 4$, $\Delta = 4\Delta_1$ si $\Delta_1 \equiv 2, 3 \bmod 4$. Soit Q une matrice entière symétrique et paire, définie positive, avec $\det Q = \Delta$. C'est la matrice donnant la forme q dans une base de L_0.

1. Séries thêta à une variable. On a défini (IV.1) des réseaux L_a de S associés aux idéaux $\mathfrak{M}_a$ de C, et pour $n \in \mathbf{N}^*$, des matrices colonnes à $(l+1)^2$ lignes $m^0_l(n, L_a)$. Pour $\tau \in \mathbf{C}$, $\mathrm{Im}\ \tau > 0$, on pose $\vartheta_a(\tau) = \sum m^0_l(n, L_a) e^{2\pi i n\tau}$, pour n allant de 1 à ∞. Chaque coefficient $\vartheta_{a,\nu}(\tau)$ est la série thêta associée au réseau L_a muni de la forme $a \mapsto q(a)/q(L_a)$ et à un certain polynôme sphérique p_ν. Soient Q_a la matrice exprimant la forme $a \mapsto q(a)/q(L_a)$ dans une base de L_a, $\Delta_a = \det Q_a$, et N_a le niveau de Q_a.

PROPOSITION 18. *On a les égalités* $\Delta_a = N_a = \Delta$.

Démonstration. Cette assertion est locale. Les réseaux considérés étant localement semblables, on se ramène au cas du réseau L_0. Il suffit de montrer que son niveau N est égal à Δ. Il est bien connu que N divise Δ, et qu'une série thêta associée à L_0 est modulaire pour $\Gamma_0(N)$, de caractère $(\Delta/\cdot)$. Le conducteur Δ de ce caractère divise donc N. ∎

Donc les séries $\vartheta_{a,\nu}(\tau)$ sont des formes paraboliques de poids $l+2$ pour le groupe $\Gamma_0(\Delta)$, de caractère $(\Delta/\cdot)$. Remarquons que si $\mathfrak{M}_a$ et $\mathfrak{M}_\beta$

ont même ordre à droite, ils ne diffèrent que par un idéal I de K: $\mathfrak{M}_a = \mathfrak{M}_\beta I$. Alors $L_a = n_{K/\mathbb{Q}}(I)L_\beta$, d'où $\vartheta_a(\tau) = |I|^{-l}\vartheta_\beta(\tau)$. Modifions donc nos notations comme en V.4. Soit $(\mathfrak{O}_a)$, $a = 1, \dots, h'$, un système de représentants des classes d'ordres maximaux de C, et $\mathfrak{M}_a$ un idéal d'ordre à gauche $\mathfrak{O}_0$ et à droite $\mathfrak{O}_a$. On pose encore $L_a = \overline{\mathfrak{M}_a}(L_0)\mathfrak{M}_a$, et $m_l(n, L_a)$, ϑ_a les séries associées à L_a. On définit

$$m_l(n) = \big(m_l(n, L_a)\big), \quad a = 1, \dots, h',$$

$$\vartheta(\tau) = \sum m_l(n) e^{2\pi i n\tau}, \quad \text{sommé de } n = 1 \text{ à } \infty.$$

C'est une matrice colonne à $h'(l+1)^2$ lignes. Considérons la matrice de Brandt réduite $B_l(1, I)$ de caractère trivial 1.

PROPOSITION 19. *On a les égalités*

(a) *si p est premier et se décompose dans K en $\mathfrak{P}_1\mathfrak{P}_2$,*

$$\tfrac{1}{2}[B_l(1, \mathfrak{P}_1) + B_l(1, \mathfrak{P}_2)]\vartheta(\tau) = T_p\vartheta(\tau),$$

(b) *si p est premier, inerte dans K,*

$$B_l(1, p)\vartheta(\tau) = T_{p^2}\vartheta(\tau) + p^{l+1}\vartheta(\tau).$$

La démonstration utilise le théorème 2 et la réduction des matrices de Brandt. ■

COROLLAIRE. *L'espace engendré par les coefficients de $\vartheta(\tau)$ est stable par les opérateurs de Hecke T_p si $(\Delta/p) = 1$ et par T_{p^2} si $(\Delta/p) = -1$.*

2. Séries de Dirichlet. On utilise le corollaire de la proposition 15. Soit A une matrice carrée d'ordre $h'(l+1)^2$ telle que pour tout $\mathfrak{P}$, $A^{-1}B_l(1, \mathfrak{P})A = \mathrm{diag}\big(\lambda_i(\mathfrak{P})\big)$, où i varie de 1 à $h'(l+1)^2$. En se rappelant la définition de la matrice Φ_1 associée au caractère 1, par ses coefficients $c_1(I) = |I|^{(l+2)/2}B_l(1, I)$ (V.4), il est clair que $A^{-1}\Phi_1 A$ est diagonale: $A^{-1}\Phi_1 A = \mathrm{diag}(\Theta_i)$, $i = 1, \dots, h'(l+1)^2$. Posons $A^{-1}\vartheta(\tau) = (\vartheta_i)$. On a les égalités:

$$T_\mathfrak{P}\Theta_i = \lambda_i(\mathfrak{P})\Theta_i \quad \text{(proposition 17)},$$

$$T_p\vartheta_i = \tfrac{1}{2}[\lambda_i(\mathfrak{P}) + \lambda_i(\mathfrak{P}^\sigma)]\vartheta_i \quad \text{si} \quad p = \mathfrak{P}\mathfrak{P}^\sigma \text{ dans } K,$$

$$T_{p^2}\vartheta_i = \lambda_i(p)\vartheta_i - p^{l+1}\vartheta_i \quad \text{si} \quad p \text{ est inerte dans } K \quad \text{(proposition 19)}.$$

La série de Dirichlet associée à une forme de Hilbert sous la forme (D) est

$$Z(s) = \sum c(I)\,|I|^{s-(l+2)/2}, \text{ sommé sur tous les idéaux de } \mathfrak{o}_K.$$

Elle vérifie l'équation:

$$\text{(E)} \quad (2\pi)^{-2s+l+2}\Gamma(s)^2 Z(s) = \Delta^{-2s+l+2}(2\pi)^{2s-(l+2)}\Gamma(l+2-s)^2 Z(l+2-s)$$

([16], p. 126).

Supposons $\vartheta_i \neq 0$. Le problème est que ϑ_i n'est pas fonction propre des T_p pour $(\Delta/p) = -1$. Soit (f_j) une base de l'espace des formes paraboliques pour $\Gamma_0(\Delta)$, de poids $l+2$ et de caractère $(\Delta/\cdot)$, telle que f_j soit fonction propre de tous les T_p, de valeurs propres $\mu_j(p)$. Choisissons f_i un élément de cette base intervenant dans la décomposition de ϑ_i relativement à (f_j). Les égalités écrites plus haut impliquent:

$$\mu_i(p) = \tfrac{1}{2}\big(\lambda_i(\mathfrak{P}) + \lambda_i(\mathfrak{P}^\sigma)\big), \quad \text{si} \quad (\Delta/p) = 1,$$

$$\mu_i(p)^2 = \lambda_i(p) - 2p^{l+1}, \quad \text{si} \quad (\Delta/p) = -1 \quad (\text{car } T_p^2 = T_{p^2} - p^{l+1}).$$

Soit $\tilde{f}_i$ la forme parabolique suivante:

$$\tilde{f}_i(\tau) = f_i|_{l+2}\begin{pmatrix} 0 & -1 \\ \Delta & 0 \end{pmatrix}(\tau) = f_i(-1/\Delta\tau)(\sqrt{\Delta}\tau)^{-(l+2)}.$$

Il est bien connu que $\tilde{f}_i$ est fonction propre de tous les T_p, de valeurs propres $\tilde{\mu}_i(p)$. Comme

$$T_p\begin{pmatrix} 0 & -1 \\ \Delta & 0 \end{pmatrix} = \left(\frac{\Delta}{p}\right)\begin{pmatrix} 0 & -1 \\ \Delta & 0 \end{pmatrix}T_p,$$

pour p ne divisant pas Δ, on obtient $\tilde{\mu}_i(p) = (\Delta/p)\mu_i(p)$ si p ne divise pas Δ. Notons $\zeta_i(s)$, $\tilde{\zeta}_i(s)$, $Z_i(s)$ les séries de Dirichlet normalisées associées à f_i, $\tilde{f}_i$, Θ_i.

THÉORÈME 4. *Si i est tel que $\vartheta_i \neq 0$ et $\lambda_i(\mathfrak{P}) = \lambda_i(\mathfrak{P}^\sigma)$ pour tout $\mathfrak{P}$, on a l'égalité $Z_i(s) = \zeta_i(s)\,\tilde{\zeta}_i(s)$.*

Démonstration. Pour $\mathrm{Re}\, s$ assez grand, toutes ces séries sont développables en produit eulérien. Si p ne divise pas Δ, on a:

(a) si $p = \mathfrak{P}\mathfrak{P}^\sigma$ dans K (i.e. $(\Delta/p) = 1$), le produit eulérien en p dans $Z_i(s)$ est $\big(1 - \lambda_i(\mathfrak{P})p^{-s} + p^{l+1-2s}\big)^{-2}$, puisque $\lambda_i(\mathfrak{P}) = \lambda_i(\mathfrak{P}^\sigma)$ ([16], p. 44). Le produit eulérien dans $\zeta_i(s)\tilde{\zeta}_i(s)$ est $\big(1 - \mu_i(p)p^{-s} + p^{l+1-2s}\big)^{-2}$ car $\tilde{\mu}_i(p) = \mu_i(p)$, d'où l'égalité puisque $\mu_i(p) = \lambda_i(\mathfrak{P})$.

(b) si p reste premier dans K (i.e. $(\Delta/p) = -1$), le produit eulérien en p dans $Z_i(s)$ (resp. $\zeta_i(s)\tilde{\zeta}_i(s)$) est $\big(1 - \lambda_i(p)p^{-2s} + p^{2(l+1)-4s}\big)^{-1}$ (resp. $\big(1 - \mu_i(p)p^{-s} - p^{l+1-2s}\big)^{-1}\big(1 + \mu_i(p)p^{-s} - p^{l+1-2s}\big)^{-1}$), et on vérifie encore qu'ils sont égaux.

Il reste à comparer les termes pour p divisant Δ. On a l'équation fonctionnelle

$$\Delta^{s/2}(2\pi)^{-s}\Gamma(s)\zeta_i(s) = (i)^{l+2}\Delta^{(l+2-s)/2}(2\pi)^{-(l+2)+s}\Gamma(l+2-s)\tilde{\zeta}_i(l+2-s).$$

Ecrivons la même équation en échangeant f_i et $\tilde{f}_i$ et faisons le produit de ces deux équations. On trouve que le produit $\zeta_i(s)\tilde{\zeta}_i(s)$ vérifie la même

équation fonctionnelle (E) que la série $Z_i(s)$. Faisons le quotient de ces équations. On obtient:

$$\frac{Z_i(s)}{\zeta_i(s)\tilde{\zeta}_i(s)} = \frac{Z_i(l+2-s)}{\zeta_i(l+2-s)\tilde{\zeta}_i(l+2-s)}.$$

D'après la première partie de la démonstration, on a l'égalité:

$$\frac{Z_i(s)}{\zeta_i(s)\tilde{\zeta}_i(s)} = \prod_{p\mid A} \frac{(1-\mu_i(p)p^{-s})(1-\tilde{\mu}_i(p)p^{-s})}{(1-\lambda_i(p)p^{-s}+p^{l+1-2s})}.$$

Il est facile de voir que si une telle fonction $P(s)$ vérifie $P(s) = P(l+2-s)$, elle est constante, clairement égale à 1. Donc $Z_i(s) = \zeta_i(s)\tilde{\zeta}_i(s)$. ■

On a eu besoin de choisir un élément de base f_i intervenant dans ϑ_i. Démontrons pour terminer que ce choix ne change rien au théorème.

Proposition 20. *Soient f (resp. f') une forme parabolique de type (k, ε) sur $\Gamma_0(N)$ (resp. (k', ε') sur $\Gamma_0(N')$), avec $T_p f = a_p f$ (resp. $T_p f' = a'_p f'$) pour tout $p \nmid NN'$, et $k \geqslant 2$. On suppose qu'il existe un corps de nombres K galoisien sur $\boldsymbol{Q}$ tel que $a_p = a'_p$ pour presque tout p totalement décomposé dans K. Si f a de la multiplication complexe par un corps quadratique imaginaire F, on suppose que K ne contient pas F. Alors il existe un caractère de Dirichlet χ, non ramifié en dehors de NN', tel que $\chi(p) = 1$ si p est totalement décomposé dans K et tel que pour tout $p \nmid NN'$, $a_p = \chi(p)a'_p$* (on renvoie à [11] pour la définition de la multiplication complexe).

Corollaire. *Si f_i et f'_i interviennent dans ϑ_i, alors $f'_i = f_i$ ou $f'_i = \tilde{f}_i$.*

On a vu que les valeurs propres de f_i, f'_i pour T_p sont égales à $\lambda_i(\mathfrak{P})$ si p se décompose dans $K = \boldsymbol{Q}(\sqrt{A})$. Le caractère χ est alors soit 1 soit $(A/\cdot)$. Comme $f_i, \tilde{f}_i$, et f'_i sont primitives, puisque leur caractère l'est, le théorème de multiplicité 1 entraîne le corollaire. ■

Démonstration de la proposition. Soit l un nombre premier divisant NN'. D'après un théorème de Deligne ([3], p. 520), il existe des représentations ϱ et ϱ' de $G = \mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ sans $\mathrm{GL}_2(\overline{\boldsymbol{Q}}_l)$, où $\overline{\boldsymbol{Q}}$ et $\overline{\boldsymbol{Q}}_l$ sont les clôtures algébriques de $\boldsymbol{Q}$ et $\boldsymbol{Q}_l$, telles que ϱ et ϱ' sont non ramifiées en dehors de NN', et telles que si $F_{p,\varrho}$, $F_{p,\varrho'}$ sont les images par ϱ, ϱ' d'un Frobenius en p, pour $p \nmid NN'$, on a $\mathrm{Tr}F_{p,\varrho} = a_p$, $\mathrm{Tr}F_{p,\varrho'} = a'_p$. Soient $G_1 = \mathrm{Gal}(\overline{\boldsymbol{Q}}/K)$ et $H = \mathrm{Ker}(\varrho) \cap \mathrm{Ker}(\varrho')$. Ce sont des sous-groupes distingués de G. Les représentations ϱ et ϱ' sont semisimples ([11], p.13) donc leurs restrictions à G_1H/H le sont aussi. Elles ont même trace sur les Frobenius en p pour p totalement décomposé dans K. D'après le théorème de Čebotarev, ces Frobenius sont denses dans G_1H/H. Donc les restrictions de ϱ et ϱ' à G_1H sont équivalentes. On peut les supposer égales. Si $g \in G$ et $g_1 \in G_1H$, on a $gg_1g^{-1} \in G_1H$, donc $\varrho(gg_1g^{-1}) = \varrho'(gg_1g^{-1})$. D'où

$$\varrho'(g)^{-1}\varrho(g)\varrho(g_1) = \varrho(g_1)\varrho'(g)^{-1}\varrho(g).$$

Donc $\varrho'(g)^{-1}\varrho(g)$ commute à $\varrho(G_1H)$. D'après nos hypothèses sur K, ϱ restreinte à G_1H est irréductible ([11], p. 22). Donc $\varrho'(g)^{-1}\varrho(g)$ est un scalaire $\chi(g)$, et χ est un caractère de G/G_1H. Par l'isomorphisme du corps de classes, on l'identifie à un caractère de Dirichlet. On a alors, pour tout $p \nmid NN'$, $\mathrm{Tr}F_{p,\varrho} = \chi(p)\mathrm{Tr}F_{p,\varrho'}$, d'où la conclusion. ■

Remarquons que, si $\vartheta_i \neq 0$, ϑ_i est dans l'espace engendré par f_i et $\tilde{f}_i$. Il est clair que $\tilde{\vartheta}_i$ est dans le même espace. Si on démontrait que ϑ_i et $\tilde{\vartheta}_i$ ne sont pas proportionnels, on en déduirait que l'espace engendré par ϑ_i et $\tilde{\vartheta}_i$ est stable par tous les opérateurs de Hecke. Malheureusement, cette non-proportionnalité ne semble pas évidente.

Bibliographie

[1] Z. I. Borevitch, I. R. Chafarevitch, *Théorie des nombres*, Monographies internationales de math. modernes, Gauthier-Villars, 1967.

[2] N. Bourbaki, *Algèbre*, chapitre 8, Hermann, 1958.

[3] P. Deligne, J. P. Serre, *Formes modulaires de poids* 1, Ann. Scient. Ec. Norm. Sup., 4ème série, 7 (1974), p. 507–530.

[4] M. Eichler, *Quadratische Formen und orthogonale Gruppen*, Springer, 1952.

[5] — *The basis problem for modular forms and the traces of the Hecke operators*, dans *Modular functions of one variable I* (Antwerp 1972), p. 75–152, L. N. 320, Springer, 1973.

[6] — *Theta functions over $\boldsymbol{Q}$ and over $\boldsymbol{Q}(\sqrt{q})$*, non publié.

[7] — *On theta functions of real algebraic number fields*, Acta Arith. 33 (1977), p. 269–292.

[8] H. Naganuma, *On the coincidence of two Dirichlet series associated with cusp forms of Hecke's "Nebentype" and Hilbert modular forms over real quadratic fields*, Journ. Math. Soc. Japan (4), 25 (1973), p. 547–555.

[9] A. P. Ogg, *Modular forms and Dirichlet series*, W. A. Benjamin Publ., New-York 1969.

[10] M. Peters, *Ternäre und quaternäre quadratische Formen und Quaternionenalgebren*, Acta Arith. 15 (1969), p. 329–365.

[11] K. Ribet, *Galois representations attached to eigenforms with Nebentypus*, dans *Modular functions of one variable V* (Bonn 1976), p. 17–52, L.N. 601, Springer, 1977.

[12] H. Shimizu, *On traces of Hecke operators*, Journ. Fac. Sci. Univ. Tokyo 10 (1963), p. 1–19.

[13] J. Tate, *Fourier analysis in number fields and Hecke's Zeta-functions* (thèse), dans J. W. S. Cassels, A. Fröhlich, *Algebraic number theory*, p. 305–347, Academic Press, Londres et New-York, 1967.

[14] M. F. Vignéras, *Représentation des opérateurs de Hecke dans les espaces de séries thêta*, non publié.

[15] N. Ja., Vilenkin, *Fonctions spéciales et théorie de la représentation des groupes*, Mono. univ. de math., Dunod, Paris 1969.

[16] A. Weil, *Dirichlet series and automorphic forms*, L.N. 189, Springer, 1971.

Reçu le 11. 1. 1978 (1022)