ACTA ARITHMETICA
XXXVII (1980)

On symmetric and unsymmetric theta functions over a real quadratic field

by

MARTIN EICHLER (BASEL)

To the memory of Paul Turán

Introduction. In the following we consider Hilbert modular forms over a real quadratic field $k = Q(\sqrt{q})$ of discriminant $q = 8$ or an odd prime $q \equiv 1 \bmod 4$. We shall further assume that k has ideal class number 1. All what will be said will certainly be true for more general quadratic fields with more or less modifications, but we think it useful to treat the simplest case first. The modular forms to be considered are those with respect to the group

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}: \quad \alpha\delta - \beta\gamma = 1, \ \alpha \in \mathfrak{o}, \ \beta \in q^{-1/2}\mathfrak{o}, \ \gamma \in q^{1/2}\mathfrak{o}, \ \delta \in \mathfrak{o}$$

where $\mathfrak{o}$ is the maximal order of k.

All modular forms will turn out to be linear combinations of theta series in the sense of Kloosterman and Schoeneberg which were studied in [3], and of which we now repeat the definition. Let K be the quaternion algebra ramified only at the infinite spots of k and $\mathfrak{M}_1, \ldots, \mathfrak{M}_H$ ideals with a common maximal left order $\mathfrak{O}$ which represent all left classes. The right orders of the $\mathfrak{M}_i$ are $\mathfrak{O}_i$. For a given integral ideal $\mathfrak{m} = (\mu)$ of k we form all integral ideals

$$\mathfrak{M} = \mathfrak{M}_i^{-1}\mathfrak{M}_j M, \qquad M \in K \tag{1}$$

of norm $\mathfrak{m}$ and left orders $\mathfrak{O}_i$ and given left class. For a certain representation $R_l(M)$ of the multiplicative group $K^\times$ of degree $(l+1)^2$ introduced in [3] we form the sums

$$B_{ij}(\mathfrak{m}) = \sum R_l(M) e_j^{-1}$$

extended over all $\mathfrak{M}$ in (1) where e_j is the index of the unit group of $\mathfrak{o}$ in that of $\mathfrak{O}_j$. The $B_{ij}(\mathfrak{m})$ are arranged in $H(l+1)^2$-rowed matrices $B_l(\mathfrak{m})$, the Brandt matrices, which are equivalent to the representations of the Hecke operators $T_{l+2}(\mathfrak{m})$ in the spaces of integral modular forms of weight 2 if $l = 0$ or of cusp forms of weight $l+2$ for $l > 0$. The Kloosterman–Schoeneberg theta series are

$$\Theta_l(z_1, z_2) = \sum B_l(\mu)\, e^{2\pi i(z_1\mu + z_2\mu^\sigma)} \tag{2}$$

summed over $\mu = 0$ and all totally positive integral μ (σ is the canonical automorphism of k).

THEOREM 1. *If the ideal class number of k is 1, all integral modular forms of weight 2 and all cusp forms of weight $l+2$ are linear combinations of coefficients of the matrix series* (2).

The proof has been given in [4] for $l > 0$. It consists of the comparison of the traces of the $B_l(\mathfrak{m})$ and of the $T_{l+2}(\mathfrak{m})$ which have been determined by Shimizu [12]. Recently Ishikawa [6] has calculated the traces of the $T_2(\mathfrak{m})$ in the cusp forms. His formula consists of two summands the second of which is, with the $-$ sign the trace of $T_2(\mathfrak{m})$ in the Eisenstein series. Thus the first summand is the trace in the space of all integral modular forms, and this is equal to the trace of the $B_0(\mathfrak{m})$.

If the ideal class number of $\boldsymbol{Q}(\sqrt{d})$ (where d is allowed arbitrary) is > 1, the $B_l(\mathfrak{m})$ and $T_{l+2}(\mathfrak{m})$ do not span a ring over $\boldsymbol{Z}$, and certain other Brandt matrices $A_l(\mathfrak{m})$ and Hecke operators $V_{l+2}(\mathfrak{m})$ have been introduced in [3] to complete the picture. A proof of Theorem 1 under more general conditions requires the $A_l(\mathfrak{m})$ and $T_{l+2}(\mathfrak{m})$ to be included in the comparison of the traces.

Our chief concern here are the symmetric modular forms

$$f(z_1, z_2) = f(z_2, z_1)$$

which preserve this property under all Hecke operators. We want to find all linear combinations of theta series which are symmetric in this sense. The problem can be stated in a slightly different way. The matrix (2) is diagonalized by a constant matrix G:

$$G^{-1}\Theta_l(z_1, z_2)G = \big(\operatorname{diag} \Phi_\nu(z_1, z_2)\big), \tag{3}$$

$$\Phi_\nu(z_1, z_2) = \sum \beta_\nu(\mu)\, e^{2\pi i(z_1\mu + z_2\mu^\sigma)}, \tag{4}$$

the Fourier coefficients of which are the eigenvalues of the $B_l(\mu) = B_l(\mathfrak{m})$. The symmetric theta functions are those whose Fourier coefficients are symmetric in the sense

$$\beta_\nu(\mu) = \beta_\nu(\mu^\sigma).$$

The determination of the number of linearly independent symmetric $\Phi_\nu(z_1, z_2)$ is connected with the arithmetic properties of the algebra K.

As will be shown in § 2, the canonical automorphism σ of k can be extended to K. A maximal order $\mathfrak{O}$ will be called *weakly symmetric* if

$$\mathfrak{O}^\sigma = C^{-1}\mathfrak{O}C \tag{5}$$

with some $C \in K^\times$. It will be called *strongly symmetric* if

$$\mathfrak{O}^\sigma = \mathfrak{O}. \tag{6}$$

In § 3 we will prove

THEOREM 2. *A weakly symmetric order $\mathfrak{O}$ is equivalent with a strongly symmetric one if the discriminant of k is either* 8 *or an odd prime.*

For Theorem 2 we need not assume that k has class number 1. We will see that the number of strongly symmetric $\mathfrak{O}$ is equal to the number of classes of definite quaternary quadratic forms of discriminant and reduced determinant both q which represent 1. The number of such classes has been determined by Kitaoka [7]. It can be conjectured that, for more general quadratic fields, the maximal orders can be divided into genera, and that Theorem 2 holds for one of the genera.

Returning to the symmetric modular forms, we shall further prove

THEOREM 3. *The number of linearly independent symmetric modular forms of weight 2 is equal to the number of classes of* (*weakly*) *symmetric maximal orders in K.*

The number of linearly independent symmetric modular forms can be obtained by specialization of a much more far reaching theorem of Saito [11], if $l > 0$. It has also been determined for arbitrary $k = \boldsymbol{Q}(\sqrt{d})$ by Busam [1], but his number is in our notation $\frac{1}{2}(h+H)$. On the other hand, our method employed in the proof of Theorem 3 can also be extended to higher weights. The complications caused by the units of finite order can certainly be handled.

Our last question concerns the unsymmetric functions $\Phi_\nu(z_1, z_2)$. As pointed out by Peters [8], Ponomarev [9], [10], and the autor [2], [3] there is a bijection between the classes of maximal orders $\mathfrak{O}$ of K and the classes of maximal lattices $\mathfrak{L}$ in a space S. This connection leads to an action of the Brandt matrices $B_l(\mu)$ on the row vectors $\vartheta_l(\tau)$ of theta functions (with spherical weight functions) as factors on the right. Now, together with (3), these theta functions are transformed simultaneously

$$\vartheta_l(\tau)G = \big(\ldots, \varphi_\nu(\tau), \ldots\big) \tag{7}$$

with components

$$\varphi_\nu(\tau) = \sum_m \lambda_\nu(m)\, e^{2\pi i m\tau}. \tag{8}$$

The $\Phi_\nu(z_1, z_2)$ in (4) which are symmetric are the Naganuma lifts of the

$\varphi_\nu(\tau)$ with the same ν, unless the latter are zero. Today it is an open question when $\varphi_\nu(\tau)=0$ in the symmetric case. But we will prove

THEOREM 4. *If $\Phi_\nu(z_1, z_2)$ is not symmetric, the $\varphi_\nu(\tau)$ with the same ν vanishes.*

This statement is both an interesting application of the "lifting theory" which has today so much publicity, and an explicit description of a large class of linear relations between theta series of which only particular examples have been known so far while many more actually do exist

§ 1. The symmetry of the Brandt matrices. In § 1 we restrict ourselves to the case $l=0$. Now $B_{ij}(\mathfrak{m})$ is the number of integral ideals (1). Let $\mathfrak{M}'_i = \mathfrak{M}_i C_i$ be another system representing the left classes and

$$\mathfrak{M}' = \mathfrak{M}_i'^{-1}\mathfrak{M}_j' M' = C_i^{-1}(\mathfrak{M}_i^{-1}\mathfrak{M}_j C_j M' C_i^{-1})C_i$$

run over all integral ideals of norm $\mathfrak{m}$. Then (1) holds with $M = C_j M' C_i^{-1}$, and the coefficients $B_{ij}(\mathfrak{m})$ of $B_0(\mathfrak{m})$ are independent of the class representations.

Let us assume that the right orders $\mathfrak{O}_1, \ldots, \mathfrak{O}_h$ be weakly symmetric, while $\mathfrak{O}_{h+1}^\sigma \cong \mathfrak{O}_{h+2}, \ldots$ Under this assumption we have

$$B_0(\mathfrak{m}^\sigma) = P_0^{-1} B_0(\mathfrak{m}) P_0 \tag{9}$$

where P_0 is a permutation matrix fixing the indices $1, \ldots, h$ and exchanging $h+1, h+3, \ldots$ with $h+2, h+4, \ldots$ Let

$$B_0(\mathfrak{m}) G_0 = G_0 \operatorname{diag}(\beta_\nu(\mathfrak{m})). \tag{10}$$

The columns of the matrix G_0 are eigenvectors of $B_0(\mathfrak{m})$ with the eigenvalues $\beta_\nu(\mathfrak{m})$. (10) holds with the same matrix G_0 and $\mathfrak{m}^\sigma$ instead of $\mathfrak{m}$. Expressing $B_0(\mathfrak{m}^\sigma)$ in the way (9) we get

$$B_0(\mathfrak{m}) P_0 G_0 = P_0 G_0 \operatorname{diag}(\beta_\nu(\mathfrak{m}^\sigma)).$$

But $\operatorname{diag}(\beta_\nu(\mathfrak{m}^\sigma))$ is obtained from $\operatorname{diag}(\beta_\nu(\mathfrak{m}))$ by another involutorial permutation matrix P_0', and we arrive at

$$B_0(\mathfrak{m}) P_0 G_0 P_0' = P_0 G_0 P_0' \operatorname{diag}(\beta_\nu(\mathfrak{m})). \tag{11}$$

By Theorem 1 the matrices $B_0(\mathfrak{m})$ span the same semisimple commutative ring as the representations $T_2(\mathfrak{m})$ of the Hecke operators in the space of integral modular forms, and the $B_0(\mathfrak{m})$ and the $T_2(\mathfrak{m})$ have the same traces. Therefore the $B_0(\mathfrak{m})$ span a ring of rank H, and then the comparison of (10) and (11) implies that

$$G_0 = c P_0 G_0 P_0'$$

with a scalar factor c, or

$$P_0' = P_0'^{-1} = G_0^{-1} P_0 G_0.$$

Comparing the traces of P_0 and P_0' we see that P_0' leaves exactly h eigenvalues $\beta_\nu(\mathfrak{m})$ fixed:

$$\beta_\nu(\mathfrak{m}^\sigma) = \beta_\nu(\mathfrak{m}) \quad \text{for } \nu = 1, \ldots, h,$$

and no other indices. This was contended in Theorem 3.

§ 2. The metric space over Q and its similarities. We consider the Witt class of quadratic forms

$$x_1^2 - qx_2^2 + f_q(x_3, \ldots, x_6)$$

where f_q is the norm form of the definite quaternion algebra K_q over Q which is ramified at ∞ and q. This class contains a quaternary definite form in 4 variables (see [2], Satz 23.3) of discriminant q. The metric space attached to this form will be called S. We will consider maximal lattices $\mathfrak{L} \subset S$ of rank 4 and norm 1. Under our assumption the reduced determinants of these lattices are equal to q. They all belong to the same ideal complex.

LEMMA 1. *There exists in S a maximal lattice $\mathfrak{L}_2$ of rank 4 and norm 1 which contains a binary sublattice of norm form equivalent with x^2+y^2. There also exists a lattice $\mathfrak{L}_3$ of rank 4 and norm 1 in S which contains a sublattice of norm from x^2+xy+y^2.*

Proof. We show at first that S contains the binary subspace $(1,1)$ (short for a space with norm form x^2+y^2). This is the case if and only if there exists a binary space B_2 such that the Witt classes of $(1, -q)+f_q$ and $(1,1)+B_2$ are the same. An equivalent expression is: the Witt class

$$(1, -q)+f_q+(-1, -1) \sim (-1, -q)+f_q$$

contains a binary space. This in turn is equivalent with the statement: f_q represents the binary form $(1, q)$. And eventually, this is the case if and only if $Q(\sqrt{-q})$ is a splitting field of the quaternion algebra K_q which is indeed the case.

Similarly we show that S contains the binary space $(1, 3)$. The analogue considerations lead to the necessary and sufficient condition that $Q(\sqrt{-3q})$ is a splitting field of K_q which is also the case.

In these two cases S contains a binary lattice of norm form x^2+y^2 and also one of norm form x^2+xy+y^2. Both binary lattices can be extended to maximal lattices of rank 4 and norm 1.

The second Clifford algebra of S can be identified with the quaternion algebra K/k which is only ramified at the infinite spots of k (see [4], [8], [9]). The orders $\mathfrak{O} \subset K$, generated over Z by all products $\mathfrak{a}_1 \ldots \mathfrak{a}_{2r}$ of vectors in a maximal lattice $\mathfrak{L}$ of norm 1 are maximal orders. If the $\mathfrak{L}_\nu$ represent all isomorphy classes of maximal lattices the $\mathfrak{O}_\nu$ attached to them represent all types of maximal orders.

The scalar products of vectors $\mathfrak{a}, \mathfrak{b} \in S$ will be written $(\mathfrak{a}, \mathfrak{b})$ and

$$\tfrac{1}{2}(\mathfrak{a}, \mathfrak{a}) = n(\mathfrak{a}).$$

The g.c.d. of $n(\mathfrak{a})$ for all $\mathfrak{a}$ contained in the lattice $\mathfrak{L}$ is the norm of $\mathfrak{L}$: $n(\mathfrak{L})$.

Elements of the second Clifford algebra K will be denoted by capital Roman letters. Vectors will often be considered as elements of the first Clifford algebra. As such they satisfy the equations $\mathfrak{a}\mathfrak{a} = \mathfrak{a}^2 = n(\mathfrak{a})$.

We are especially interested in "unit" vectors $\mathfrak{e}$ of norm $n(\mathfrak{e}) = 1$. They can all be transformed into each other by isometries of S. Therefore we may assume that a system of class representatives $\mathfrak{L}_\nu$ of lattices, containing unit vectors, contain all the same vector $\mathfrak{e}$. This $\mathfrak{e}$ will be kept fixed throughout.

As an element of the first Clifford algebra, $\mathfrak{e}$ defines an isomorphism of K by

$$M \to \mathfrak{e}^{-1}M\mathfrak{e} = \mathfrak{e}M\mathfrak{e} = M^\sigma$$

for all $M \in K$. In k it induces the canonical isomorphism.

The canonical antiautomorphism $\varkappa$ of K is defined by

$$M^\varkappa = S_{K/k}(M) - M = MN_{K/k}(M)^{-1}.$$

It commutes with σ.

If $\mathfrak{c} \neq 0$ is an arbitrary vector of S, the order $\mathfrak{c}^{-1}\mathfrak{O}\mathfrak{c} = \mathfrak{O}'$ is attached to the lattice

$$\mathfrak{c}^{-1}\mathfrak{L}\mathfrak{c} = n(\mathfrak{c})^{-1}\mathfrak{c}\mathfrak{L}\mathfrak{c} = \mathfrak{L}' \tag{12}$$

whose vectors $\mathfrak{a}'$ are obtained from the $\mathfrak{a} \in \mathfrak{L}$ by the reflection

$$\mathfrak{a}' = n(\mathfrak{c})^{-1}\mathfrak{c}\mathfrak{a}\mathfrak{c} = \mathfrak{a} - \frac{(\mathfrak{a}, \mathfrak{c})}{n(\mathfrak{c})}\mathfrak{c} \tag{13}$$

at the 3-space orthogonal to $\mathfrak{c}$.

LEMMA 2. *To the lattices $\mathfrak{L}_2, \mathfrak{L}_3$ in Lemma* 1 *containing the vector* $\mathfrak{e}$ *strongly symmetric orders $\mathfrak{O}_2, \mathfrak{O}_3$ of K are attached which contain units U_2, U_3 of orders* 4 *and* 3 *with the property*

$$U_i^\sigma = U_i^{-1} \quad (i = 2, 3). \tag{14}$$

Proof. As already mentioned, the assumption $\mathfrak{e} \in \mathfrak{L}_i$ does not restrict the generality. Then $\mathfrak{O}_i^\sigma = \mathfrak{e}^{-1}\mathfrak{O}_i\mathfrak{e} = \mathfrak{O}_i$. From Lemma 1 follows that $\mathfrak{L}_2, \mathfrak{L}_3$ contain further unit vectors $\mathfrak{e}_2, \mathfrak{e}_3$ such that $U_2 = \mathfrak{e}\mathfrak{e}_2$ and $U_3 = \mathfrak{e}\mathfrak{e}_3$ are units of $\mathfrak{O}_i$. Now (14) is evident. Because $\mathfrak{e}$ and $\mathfrak{e}_2$ are orthogonal, we see that $U_2^2 = -1$. And because $n(x\mathfrak{e} + y\mathfrak{e}_3) = x^2 + xy + y^2$ we have $U_3^3 = 1$.

LEMMA 3. *Let $q \neq 8$ and the lattice given by* (12): $\mathfrak{L}' = \mathfrak{L}$. *If the vector* $\mathfrak{c}$ *is assumed to be a primitive vector in $\mathfrak{L}$, its norm is either* 1 *or q. In the latter case it is contained in the complementary lattice $q\mathfrak{L}^*$ where $\mathfrak{L}^*$ is defined by $(\mathfrak{L}, \mathfrak{L}^*) \subseteq \mathbf{Z}$.*

Proof. According to the assumption $n(\mathfrak{c})$ divides all products $(\mathfrak{a}, \mathfrak{c})$, and thus either $n(\mathfrak{c}) = 1$ or $n(\mathfrak{c}) = q$ and $(\mathfrak{L}, q^{-1}\mathfrak{c}) \subseteq \mathbf{Z}$.

LEMMA 4. *Let $q \neq 8$ and the lattices $\mathfrak{L}, \mathfrak{L}'$ connected in the way* (12). *Furthermore assume the orders of these lattices connected by*

$$\mathfrak{O}' = C^{-1}\mathfrak{O}C$$

with a $C \in \mathfrak{O}$ of norm 2. *If again $\mathfrak{c}$ is assumed to be a primitive vector in $\mathfrak{L}$, it has either norm* 2 *or* $2q$. *In the latter case $\mathfrak{c}$ is contained in $q\mathfrak{L}^*$.*

Proof. Under the assumptions we have $2\mathfrak{O}' \subset \mathfrak{O}$, and $n(\mathfrak{c})$ divides all products $2(\mathfrak{a}, \mathfrak{c})$ $n(\mathfrak{c})$ cannot be odd because, otherwise, $\mathfrak{L}' = \mathfrak{L}$. Thus we have either $n(\mathfrak{c}) = 2$ or $2q$.

§ 3. Proof of Theorem 2. In § 3 the class number of k need not be 1. We omit the cases $q = 8$ and $q = 5$ when all maximal lattices and therefore all maximal orders $\mathfrak{O}$ belong to the same class (resp. type), and these $\mathfrak{O}$ are strongly symmetric. We assume that $\mathfrak{O}$ satisfies (5). Applying σ to (5) we obtain $\mathfrak{O} = (CC^\sigma)^{-1}\mathfrak{O}(CC^\sigma)$ which implies

$$CC^\sigma = \alpha U \tag{15}$$

with $\alpha \in k$ and a unit $U \in \mathfrak{O}$. If U is not contained in k, the Dirichlet unit theorem allows for U the following possibilities:

1) U has orders 5 or 10 or 8.
2) U^2 is a totally negative unit in k.
3) U has orders 3 or 4 or 6.

The cases 1) are only possible for $q = 5$ or 8 which have been excluded. In case 2 U^2 must be $-\varepsilon^{2h}$ with the fundamental unit ε of k, and then $U = V\varepsilon^h$, $V^2 = -1$, contrary to the assumption.

Now we assume U to have order 3. The maximal order $\mathfrak{O}_3$ mentioned in Lemma 2 contains a U_3 of order 3 with $U_3^\sigma = U_3^{-1}$. Let $A^{-1}UA = U_3$. Then we can treat $\mathfrak{O}' = A^{-1}\mathfrak{O}A$ instead of $\mathfrak{O}$ and therefore assume without loss of generality $U = U_3$ and $U^\sigma = U^{-1}$. This implies

$$U = U^{2(1-\sigma)} = U^2(U^{-2})^\sigma. \tag{16}$$

Furthermore from (15)

$$C^\sigma C = \alpha C^{-1}UC = \alpha^\sigma U^\sigma = \alpha^\sigma U^{-1},$$

whence

$$C^{-1}UC = \alpha^{\sigma-1}U^{-1} \tag{17}$$

and $\alpha^{3(1-\sigma)} = 1$ and even $\alpha^{1-\sigma} = 1$. Then

$$C^{-1}UC = U^{-1}$$

and from (15), (16), (17)

$$U^{-2}C(CU^2)^\sigma = U^{-2}C(U^{-2}C)^\sigma = a.$$

Since we may replace C by $U^{-2}C$ in (5), we have been led to the case $U = 1$.

If $U = 1$, C and C^σ in (15) commute. If they lie in k, $\mathfrak{O}$ is strongly symmetric. If not, $k(C)$ is invariant under σ and therefore

$$k(C) = Q(\sqrt{q}, M), \qquad M^\sigma = M, \qquad M^2 = -m < 0, \qquad \in Q.$$

Let

$$C = \beta+\gamma M, \qquad C^\sigma = \beta^\sigma+\gamma^\sigma M, \qquad (\beta, \gamma \in k).$$

Then

$$CC^\sigma = \beta\beta^\sigma - m\gamma\gamma^\sigma + (\beta\gamma^\sigma+\beta^\sigma\gamma)M = a \in Q.$$

Therefore $\beta\gamma^\sigma = -\beta^\sigma\gamma = -(\beta\gamma^\sigma)^\sigma$ and with some $b \in Q$:

$$\beta\gamma^\sigma = b\sqrt{q}, \qquad C = (\beta\beta^\sigma - b\sqrt{q}M)\beta^{-\sigma}.$$

We replace C by $C\beta^{-\sigma}$ and have then $C = a - b\sqrt{q}M$ with $a, b \in Q$. Now we see that

$$C^\varkappa = C^\sigma \tag{18}$$

where $\varkappa$ is the canonical antiautomorphism.

Such a C can be written as a product of two vectors one of which is $\mathfrak{e}$: $C = \mathfrak{c}\mathfrak{e}$. Indeed we have $C\mathfrak{e} = \mathfrak{c}+B$ where B is the product of 3 orthogonal vectors. Application of $\varkappa$ leads to $\mathfrak{e}C^\varkappa = \mathfrak{c}-B$, and (18) to

$$\mathfrak{c}-B = \mathfrak{e}C^\varkappa = \mathfrak{e}C^\sigma = C\mathfrak{e} = \mathfrak{c}+B$$

or $B = 0$ and

$$C = \mathfrak{c}\mathfrak{e}.$$

Now we find

$$\mathfrak{O}^\sigma = \mathfrak{e}^{-1}\mathfrak{O}\mathfrak{e} = \mathfrak{e}^{-1}\mathfrak{c}^{-1}\mathfrak{O}\mathfrak{c}\mathfrak{e}$$

and $\mathfrak{O} = \mathfrak{c}^{-1}\mathfrak{O}\mathfrak{c}$, and then

$$\mathfrak{L} = \mathfrak{c}^{-1}\mathfrak{L}\mathfrak{c}.$$

Let $\mathfrak{c} = f\mathfrak{c}_0$ with a primitive vector $\mathfrak{c}_0$ in $\mathfrak{L}$ and f a factor in Q. Due to Lemma 3, $n(\mathfrak{c}_0) = 1$ or q. On the other hand, $CC^\sigma = f^2 n(\mathfrak{c}_0)$. Since $q = n(\varepsilon\sqrt{q})$, $CC^\sigma = n(\delta)$ for some $\delta \in k$. Replacing C by $C\delta^{-1}$ we obtain $CC^\sigma = 1$, and then

$$C = (1+C)^{1-\sigma}.$$

Now $\mathfrak{O}' = (1+C)^{-1}\mathfrak{O}(1+C)$ is strongly symmetric.

At last we have to treat the case $U^2 = -1$ in (15). Let $\mathfrak{O}_2$ be the order mentioned in Lemma 2 containing a unit U_2 with $U_2^2 = -1$, $U_2^\sigma = U_2^{-1}$, and $U_2 = A^{-1}UA$. We replace $\mathfrak{O}$ by $A^{-1}\mathfrak{O}A$ and can therefore assume without loss of generality that $U^\sigma = U^{-1} = -U$. From (15) we deduce again (17), and $a^{2(1-\sigma)} = 1$ or $a^{1-\sigma} = \pm 1$. In the case of the lower sign,

(17) implies that C and U commute. Now we find, using $U = (1+U)^{1-\sigma}$,

$$C(1+U)\big(C(1+U)\big)^\sigma = 2CC^\sigma = 2a,$$

and hence $a^\sigma = a$, a contradiction.

Thus we have $a^\sigma = a$ for which we write a, an element of Q. From (17)

$$C^{-1}UC = U^{-1} = -U. \tag{19}$$

Since $U = (1+U)^{1-\sigma}$, (15) can be written

$$(1+U)^{-1}C\big(C(1+U)\big)^\sigma = a$$

and because of (19)

$$C(1+U)\big(C(1+U)\big)^\sigma = 2a, \tag{20}$$

and $\big(C(1+U)\big)^\varkappa = \pm\big(C(1+U)\big)^\sigma$. In case of the lower sign we replace C by $C\sqrt{q}$ which changes the sign. As above, there is a vector $\mathfrak{c}$ such that

$$C(1+U) = \mathfrak{c}\mathfrak{e} \qquad \text{or} \qquad C = \tfrac{1}{2}\mathfrak{c}(1+U)\mathfrak{e}$$

and

$$\mathfrak{O}^\sigma = \mathfrak{e}^{-1}\mathfrak{O}\mathfrak{e} = C^{-1}\mathfrak{O}C = \big(\mathfrak{c}(1+U)\mathfrak{e}\big)^{-1}\mathfrak{O}\big(\mathfrak{c}(1+U)\mathfrak{e}\big)$$

which leads to

$$\mathfrak{c}^{-1}\mathfrak{O}\mathfrak{c} = (1-U)^{-1}\mathfrak{O}(1-U).$$

From Lemma 4 follows $n(\mathfrak{c}) = 2f^2$ or $2qf^2$ with an $f \in Q$, and

$$C(1+U)\big(C(1+U)\big)^\sigma = 2a = 2f^2 \qquad \text{or} = 2qf^2$$

now $a = n(\delta)$ with a δ in k. Again we may replace C by $C\delta^{-1}$ and obtain

$$CC^\sigma = U. \tag{21}$$

Because $U^\sigma = -U$, and $U \in \mathfrak{O}$, also $U \in \mathfrak{O}^\sigma$. Then there exists an $\mathfrak{o}[U]$-ideal $\mathfrak{A}$ such that

$$\mathfrak{O}\mathfrak{A} = \mathfrak{A}\mathfrak{O}^\sigma.$$

Comparison with (5) yields

$$\mathfrak{O}\mathfrak{A}C^{-1} = \mathfrak{A}C^{-1}\mathfrak{O},$$

and this ambigue ideal must be $\mathfrak{O}\mathfrak{a}$ with an $\mathfrak{o}$-ideal $\mathfrak{a}$. Replacing $\mathfrak{A}$ by $\mathfrak{A}\mathfrak{a}^{-1}$ we have

$$\mathfrak{O}\mathfrak{A}C^{-1} = \mathfrak{A}C^{-1}\mathfrak{O} = \mathfrak{O}. \tag{22}$$

Here we apply σ:

$$\mathfrak{O}^\sigma\mathfrak{A}^\sigma C^{-\sigma} = \mathfrak{O}^\sigma = C^{-1}\mathfrak{O}C$$

which is (see (22))

$$C\mathfrak{O}^\sigma C^{-1}C\mathfrak{A}^\sigma C^{-\sigma}C^{-1} = \mathfrak{O}.$$

On the left we use (21) and obtain

$$\mathfrak{O}C\mathfrak{A}^{\sigma} = \mathfrak{O}.$$

But because of (19): $\mathfrak{A}C^{-1} = C^{-1}\mathfrak{A}^{\sigma}$ and by (22)

$$\mathfrak{O}C\mathfrak{A}^{\sigma} = \mathfrak{O} = \mathfrak{O}C^{-1}\mathfrak{A}^{\sigma}.$$

This yields $\mathfrak{O}C = \mathfrak{O}C^{-1}$, and then C is a unit in $\mathfrak{O}$, and $\mathfrak{O}$ is strongly symmetric.

§ 4. Proof of Theorem 4. The class number of k will again be assumed to be 1. p will always denote a prime which is decomposed in k such that $p = \pi\pi^{\sigma}$, $\pi \neq \pi^{\sigma}$.

In [4] we connected the matrices $P_l(\mathfrak{m})$ which count the integral transformations mapping the lattices of norm 1 into other lattices of norm $\mathfrak{m}$ with the Brandt matrices $B_l(\mu)$ of K. We proved (the subscript l will be omitted in § 4)

$$P(p) = B(\pi) + B(\pi^{\sigma}). \tag{23}$$

Now we need a similar equation for $P(p^2)$. As pointed out in [2], the considerations there on which the present ones are based are valid if the linear transformations just mentioned are restricted to such which have given elementary divisors p, p, p, p or $1, 1, p^2, p^2$ or $1, p, p, p^2$. The respective matrices will be called $P_0(p^2)$, $P_1(p^2)$, and $P_2(p^2)$.

For the proof of (23) we used the fact that two lattices $\mathfrak{L}$, $\mathfrak{L}'$ and their orders $\mathfrak{O}, \mathfrak{O}'$ are connected in the way

$$\begin{gathered} \mathfrak{L} \to \mathfrak{M}^{\varkappa}\mathfrak{L}\mathfrak{M} = \mathfrak{L}', \\ \mathfrak{O} \to \mathfrak{O}' \quad \text{with} \quad \mathfrak{M}^{\varkappa}\mathfrak{M} = N(\mathfrak{M})\mathfrak{O}' \end{gathered} \tag{24}$$

by $\mathfrak{O}$-left ideals $\mathfrak{M}$. The norm of the similarity transformation attached to $\mathfrak{M}$ is $n_{k/Q}(N_{K/k}(\mathfrak{M}))$ (see [4], Theorem 1).

The present question is: what is the system of elementary divisors of a matrix taking a basis of $\mathfrak{L}$ into one of $\mathfrak{L}'$, if $\mathfrak{L}$ and $\mathfrak{L}'$ are connected by (24), and if $n(N(\mathfrak{M})) = p^2$? The answer can be worked out locally. For sake of simplicity we write $\mathfrak{L}, \mathfrak{O}$ etc. for their p-adic extensions.

Without loss of generality we may assume $\mathfrak{e} \in \mathfrak{L}$ and $\mathfrak{O}^{\sigma} = \mathfrak{O}$. (If necessary we can exchange $\mathfrak{e}$ for another unit vector.) The p-adic extension of the principal order $\mathfrak{o}$ of k becomes

$$\mathfrak{o} = \varepsilon_1 \boldsymbol{Z}_p \oplus \varepsilon_2 \boldsymbol{Z}_p$$

with two orthogonal idempotents $\varepsilon_1, \varepsilon_2$ which are interchanged by σ. Accordingly

$$\mathfrak{O} = \varepsilon_1 R_p \oplus \varepsilon_2 R_p$$

where R_p is the ring of the two-rowed matrices with elements in $\boldsymbol{Z}_p$.

The "symmetric" elements $A \in K$ with the property $A^{\varkappa\sigma} = A$ have been shown in § 3 to be $A = \mathfrak{e}\mathfrak{a}$ with vectors $\mathfrak{a} \in S$. It is easy to see (cf. [5], p. 630) that such $A \in \mathfrak{O}$ have $\mathfrak{a} \in \mathfrak{L}$.

Now we consider the map (24) with $\mathfrak{M} = \mathfrak{O}M$ where both sides are multiplied by $\mathfrak{e}$:

$$\mathfrak{e}\mathfrak{L} \to \mathfrak{e}\mathfrak{L}' = \mathfrak{e}M^{\varkappa}\mathfrak{L}M = M^{\varkappa\sigma}\mathfrak{e}\mathfrak{L}M. \tag{25}$$

Put $A = \varepsilon_1 A_1 + \varepsilon_2 A_2$ for an element of $\mathfrak{e}\mathfrak{L}$. Because $A^{\varkappa\sigma} = A$, it must have the form

$$A = \varepsilon_1 B + \varepsilon_2 B^{\varkappa} \quad (B = A_1).$$

With $M = \varepsilon_1 M_1 + \varepsilon_2 M_2$, (25) becomes

$$B \to B' = M_2^{\varkappa} B M_1. \tag{26}$$

In the p-adic extension of $\mathfrak{o}$, p becomes

$$p = (\varepsilon_1 p + \varepsilon_2)(\varepsilon_1 + p\varepsilon_2) = \pi\pi^{\sigma}.$$

A primitive ideal $\mathfrak{O}M$ with $N_{K/k}(M) = \pi^2$ has the local component $\varepsilon_1 M_1 + \varepsilon_2 M_2$ with M_1 a primitive matrix with determinant p^2 and M_2 a unimodular matrix. Because of (26) such an ideal generates a linear transformation $\mathfrak{L} \to \mathfrak{L}'$ with elementary divisors $1, 1, p^2, p^2$. The analogue holds for $N_{K/k}(M) = \pi^{2\sigma}$.

If $\mathfrak{M} = \mathfrak{O}\pi$, we have $M_1 = p$ times a unimodular matrix, and such an $\mathfrak{M}$ yields a linear transformation $\mathfrak{L} \to \mathfrak{L}'$ with elementary divisors p, p, p, p. The analogue holds for $\mathfrak{M} = \mathfrak{O}\pi^{\sigma}$.

Eventually if $N_{K/k}(\mathfrak{M}) = p = \pi\pi^{\sigma}$, M_1 and M_2 have both determinants p, and then (26) is a transformation $\mathfrak{L} \to \mathfrak{L}'$ with elementary divisors $1, p, p, p^2$.

The transformations $\mathfrak{L} \to \mathfrak{L}'$ and the Brandt matrices are both represented in the space of weighted numbers of representations of the natural integers n by the norm forms of these lattices as in [4], § 4. In this representation we can summarize the above considerations as

$$\begin{gathered} P_1(p^2) + 2P_0(p^2) = B(\pi^2) + B(\pi^{2\sigma}), \\ P_2(p^2) = B(p) \end{gathered} \tag{27}$$

where evidently $P_0(p^2) = p^l E$ with E the unit matrix.

Next we compare the action of the $P_i(p^2)$ on the (vectors of) theta functions $\vartheta(\tau)$ as in [4], (24). They are based on the equations

$$m(n)P_i(p^2) = \sum_{\nu} \varrho_i(\mathfrak{C}_{\nu})\, m(np^2, \mathfrak{C}_{\nu}).$$

These have been proved in [2], (18.33), and it has been mentioned that they are valid if the $P(p^2)$ are specialized to fixed systems of elementary divisors. The $\mathfrak{C}_\nu$ mean certain residue classes of $\mathfrak{L} \bmod p^2\mathfrak{L}$, and the $\varrho_i(\mathfrak{C}_\nu)$ are certain numbers attached to them (see [2], § 11.4). Their calculation is an easy task which we omit for sake of brevity. The considerations end up with

$$\vartheta(\tau)\tfrac{1}{2}\big(P_1(p^2)+P_0(p^2)\big) = \vartheta(\tau)|_{l+2}T(p^2),$$

$$\vartheta(\tau)P_2(p^2) = \vartheta(\tau)|_{l+2}T(p^2). \tag{28}$$

With (27) this is

$$\vartheta(\tau)\tfrac{1}{2}\big(B(\pi^2)+B(\pi^{2\sigma})\big) = \vartheta(\tau)B(p) = \vartheta(\tau)|_{l+2}T(p^2). \tag{29}$$

Together with (29) we need [4], (28):

$$\vartheta(\tau)\tfrac{1}{2}\big(B(\pi)+B(\pi^{\sigma})\big) = \vartheta(\tau)|_{l+2}T(p). \tag{30}$$

(We may add that (29), (30) hold also for $l = 0$ in which case $\vartheta(\tau)$ has constant terms which have not been compared on both sides. But they must also be equal because both sides are modular forms, and all coefficients $c(n)$ with $n \neq 0$ have shown to be equal.)

With this we are prepared to prove Theorem 4. We start from the functions (3) and (7) with their Fourier expansions (4) and (8), where we may assume $\beta_\nu(1) = \lambda_\nu(1) = 1$. Contrary to the theorem let $\beta_\nu(\pi) \neq \beta_\nu(\pi^\sigma)$ for some p, but $\varphi_\nu(\tau) \neq 0$. Equations (29) and (30) are now

$$\begin{aligned}\beta_\nu(\pi)+\beta_\nu(\pi^\sigma) &= 2\lambda_\nu(p),\\ \beta_\nu(\pi^2)+\beta_\nu(\pi^{2\sigma}) &= 2\beta_\nu(p) = 2\lambda_\nu(p^2).\end{aligned} \tag{31}$$

The Naganuma lift of $\varphi_\nu(\tau)$ is a symmetric eigenfunction and therefore $\Phi_\mu(z_1, z_2) = \Phi_\mu(z_2, z_1)$ for some $\mu \neq \nu$ (see for example [11] or [14]). Therefore the same equations hold for μ instead of ν while the right sides remain unchanged.

Now we form the function

$$\Psi(z_1, z_2) = \Phi_\nu(z_1, z_2)+\Phi_\nu(z_2, z_1)-2\Phi_\mu(z_1, z_2).$$

It has the following properties: (a) together with its Hecke transforms it spans a space of dimension 3, (b) its Fourier coefficients are $\gamma(\mu) = 0$ for $\mu = 1, \pi, \pi^\sigma, p, \pi^2 = \pi^{2\sigma}$ (because $\gamma(\pi^2)+\gamma(\pi^{2\sigma}) = 0$ from (31) and $\gamma(\pi^2) = \gamma(\pi^{2\sigma})$, since $\Psi(z_1, z_2) = \Psi(z_2, z_1)$).

From (b) we see that $\Psi(z)$, $\Psi(z)|T(\pi)$, $\Psi(z)|T(\pi^\sigma)$ have Fourier coefficients $\gamma(1) = 0$. Therefore they are linearly dependent. But also $\Psi(z)|T(\pi^2)$ and $\Psi(z)|T(\pi^{2\sigma})$ have $\gamma(1) = 0$. Hence the latter are linear combinations of $\Psi(z)$ and $\Psi(z)|T(\pi)$ of $\Psi(z)$ and $\Psi(z)|T(\pi^\sigma)$. This implies that the space spanned by $\Psi(z)$ and all Hecke transforms has dimension only 2, in contradiction to (a).

Literature

[1] R. Busam, *Eine Verallgemeinerung gewisser Dimensionsformeln von Shimizu*, Inventiones Math. 11 (1970), pp. 110–149.

[2] M. Eichler, *Quadratische Formen und orthogonale Gruppen*, 2. Aufl., Springer-Verlag, Berlin–Heidelberg–New York 1974.

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

[4] — *Theta functions over Q and $Q(\sqrt{q})$*, in: *Modular Functions of one Variable*, vol. VI, Lecture Notes in Mathematics, Springer-Verlag, Berlin–Heidelberg–New York 1977.

[5] — *Über definite quaternäre quadratische Formen von Primzahldiskriminante*, Comm. Pure Appl. Math. 29 (1976), pp. 623–647.

[6] H. Ishikawa, *The traces of Hecke operators in the space of 'Hilbert modular' type cusp forms of weight two*, to appear.

[7] Y. Kitaoka, *Quaternary even positive definite quadratic forms with prime discriminant*, Nagoya Math. Journ. 52 (1973), pp. 147–161.

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

[9] P. Ponomarev, *Arithmetic of quaternary quadratic forms*, ibid. 29 (1976), pp. 1–48.

[10] — *A correspondence between quadratic forms*, Nagoya Math. Journ. 62 (1976), pp. 125–140.

[11] H. Saito, *Automorphic forms and algebraic extensions of number fields*, Lecture Notes in Maths. No. 8, Kyoto Univ. 1975.

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

[13] M. F. Vigneras, *Nombre de classes d'un ordre d'Eichler et partie fractionnaire de $\zeta_k(-1)$*, Thèse Univ. de Bordeau I, 1974.

[14] D. Zagier, *Modular forms associated to real quadratic fields*, Inventiones Math. 30 (1975), pp. 1–46.

Received on 30. 7. 1977 (972)