

**REPRESENTATIONS OF QUADRATIC FORMS  
AND THEIR APPLICATION TO  
SELBERG'S ZETA FUNCTIONS**

*Dedicated to the memory of Taira Honda*

YOSHIYUKI KITAOKA

Let  $M$  and  $L$  be quadratic lattices over the maximal order of an algebraic number field. In case of dealing with representations of  $M$  by  $L$ , they sometimes assume certain indefiniteness and the condition  $\text{rank } L - \text{rank } M \geq 3$ . In this case, representation problems are reduced not to global but to local problems by virtue of the strong approximation theorem for rotations and of the fact that for regular quadratic spaces  $U, V$  over a non-archimedean local field there is an isometry from  $U$  to  $V$  if  $\dim V - \dim U \geq 3$ . On the contrary, global properties seem to be strongly concerned if we omit one of those two assumptions. As an example we prove in §1 that there is a sublattice of codimension 1 which characterizes  $L$  in a certain sense. In §2 we prove as its application that certain Selberg's zeta functions are linearly independent.

We denote by  $\mathbf{Q}, \mathbf{Z}, \mathbf{Q}_p$  and  $\mathbf{Z}_p$  the rational number field, the ring of rational integers, the  $p$ -adic completion of  $\mathbf{Q}$ , and the  $p$ -adic completion of  $\mathbf{Z}$ . We mean by a quadratic lattice  $L$  over  $\mathbf{Z}$  (resp.  $\mathbf{Z}_p$ ) a  $\mathbf{Z}$  (resp.  $\mathbf{Z}_p$ )-lattice in a regular quadratic space  $U$  over  $\mathbf{Q}$  (resp.  $\mathbf{Q}_p$ ), and by definition  $\text{rank } L = \dim U$ . For a quadratic lattice  $L$  over  $\mathbf{Z}$  (or  $\mathbf{Z}_p$ ) we denote by  $Q(x)$  and  $B(x, y)$  the quadratic form and the bilinear form associated with  $L$  ( $2B(x, y) = Q(x + y) - Q(x) - Q(y)$ ), and by  $dL$  the determinant of  $(B(e_i, e_j))$  where  $\{e_i\}$  is a basis of  $L$  over  $\mathbf{Z}$  (or  $\mathbf{Z}_p$ ).  $dL$  is uniquely determined for a quadratic lattice  $L$  over  $\mathbf{Z}$ , and for a quadratic lattice  $L$  over  $\mathbf{Z}_p$ ,  $dL$  is unique up to the squares of units in  $\mathbf{Z}_p$ . For two ordered sets  $(a_1, a_2, \dots, a_n), (b_1, b_2, \dots, b_n)$ , we define the order  $(a_1, a_2, \dots, a_n) \leq (b_1, b_2, \dots, b_n)$  by either  $a_i = b_i$  for  $i < k$  and  $a_k < b_k$  for some  $k \leq n$

---

Received November 18, 1975.

or  $a_i = b_i$  for any  $i$ .

Let  $L$  be a quadratic lattice over  $\mathbf{Z}_p$ ; then  $L$  has a Jordan splitting  $L = L_1 \perp L_2 \perp \cdots \perp L_k$ , where  $L_i$  is a  $p^{a_i}$ -modular lattice and  $a_1 < a_2 < \cdots < a_k$ . We denote by  $t_p(L)$  the ordered set  $(\underbrace{a_1, \cdots, a_1}_{\text{rank } L_1}, \cdots, \underbrace{a_k, \cdots, a_k}_{\text{rank } L_k})$ .

For simplicity we denote  $t_p(\mathbf{Z}_p L)$  by  $t_p(L)$  for a quadratic lattice  $L$  over  $\mathbf{Z}$ .

**§1. LEMMA.** *Let  $L$  be a  $\mathbf{Z}_p$ -lattice in a regular quadratic space  $U$  over  $\mathbf{Q}_p$ ; then  $L$  has a  $\mathbf{Z}_p$ -submodule<sup>\*)</sup>  $M$  satisfying the following conditions 1), 2):*

1)  $dM \neq 0$ ,  $\text{rank } M = \text{rank } L - 1$ , and  $M$  is a direct summand of  $L$  as a module.

2) Let  $L'$  be a  $\mathbf{Z}_p$ -lattice in  $U$  containing  $M$ ; then  $L' = L$  if  $dL' = dL$ , and  $t_p(L') \geq t_p(L)$ .

*Proof.* Firstly we assume that  $L$  is modular; then we may assume that  $L$  is unimodular without loss of generality by scaling. Let  $L'$  be a lattice in question in 2); then  $dL' = dL$ ,  $t_p(L') \geq t_p(L)$  imply that  $L'$  is also unimodular. Suppose that  $L$  has an orthogonal base, that is,

$L = \prod_{i=1}^n \mathbf{Z}_p v_i$ . We put  $M = \prod_{i=1}^{n-1} \mathbf{Z}_p v_i$ ; then  $M$  satisfies 1), and  $M$  is unimodular. Hence  $M$  splits  $L'$  and  $L' = M \perp a\mathbf{Z}_p v_n$  for  $a \in \mathbf{Q}_p$ . Since  $L'$  is unimodular,  $a$  is a unit. This means  $L' = L$ . If  $L$  does not have an orthogonal base, then  $p = 2$  and  $L = \prod_{i=1}^k \mathbf{Z}_2[u_i, v_i]$ , where  $\mathbf{Z}_2[u_i, v_i] \cong$

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  for  $i < k$ , and  $\mathbf{Z}_2[u_k, v_k] \cong \begin{pmatrix} 2c & 1 \\ 1 & 2c \end{pmatrix}$  ( $c = 0$  or  $1$ ). Put  $M = \prod_{i=1}^{k-1} \mathbf{Z}_2[u_i, v_i] \perp \mathbf{Z}_2[u_k + v_k]$ ; then  $Q(u_k + v_k) = 4c + 2 \neq 0$  implies  $dM \neq 0$ . The rest of 1) is obvious. Since a unimodular lattice  $\prod_{i=1}^{k-1} \mathbf{Z}_2[u_i, v_i]$  splits  $L, L'$  and

$M$ , we may assume  $k = 1$  to prove 2). Now we have  $L = \mathbf{Z}_2[u, v]$ ,  $M = \mathbf{Z}_2[u + v]$ , where  $Q(u) = Q(v) = 2c$ ,  $B(u, v) = 1$ , and  $L'$  is a unimodular lattice containing  $u + v$ . Since  $Q(u + v) = 2(2c + 1)$ ,  $u + v$  is maximal in  $L'$ . Hence  $L' = \mathbf{Z}_2[u + v, au + bv]$  for some  $a, b$  in  $\mathbf{Q}_2$ . From the assumption that  $L'$  is unimodular follows that  $B(u + v, au + bv) = (a + b)(2c + 1)$  is a unit and  $Q(au + bv) = 2c(a^2 + b^2) + 2ab$  is in  $\mathbf{Z}_2$ . Put  $a + b = x$ ; then  $x$  is a unit.  $Q(au + bv) = 2(2c - 1)a^2 - 2(2c - 1)ax$

<sup>\*)</sup> We mean a finitely generated module by a module for brevity in this paper.

$+ 2cx^2 \in \mathbf{Z}_2$  implies  $a \in \mathbf{Z}_2$ . Hence we get  $a, b \in \mathbf{Z}_2$ , and  $L' = L$ . Coming back to general cases, let  $L$  be a quadratic lattice and  $L = \perp_{i=1}^k L_i$ , where  $L_i$  is  $p^{a_i}$ -modular and  $a_1 < \dots < a_k$ . Denote by  $M_k$  a submodule of  $L_k$  which satisfies 1), 2) in case of  $L = L_k$  in Lemma and put  $M = \perp_{i=1}^{k-1} L_i \perp M_k$ . Obviously  $M$  satisfies the condition 1). Let  $L'$  be a lattice in question in 2); then from the assumptions  $t_p(L') \geq t_p(L)$ ,  $L' \supset M$  follows that  $L_1$  splits  $L, M$  and  $L'$  (82: 15 in [2]). Hence we have only to prove the Lemma for the orthogonal complements of  $L_1$  in  $L, L'$  and  $M$ . By induction it suffices to prove it in case of  $k = 1$ . This was proved firstly.

We call  $M$  a characteristic submodule of  $L$ .

**THEOREM.** *Let  $L$  be a  $\mathbf{Z}$ -lattice in a regular quadratic space  $U$  over  $\mathbf{Q}$ ; then  $L$  has a  $\mathbf{Z}$ -submodule  $M$  satisfying the following conditions 1), 2):*

1)  $dM \neq 0$ ,  $\text{rank } M = \text{rank } L - 1$ , and  $M$  is a direct summand of  $L$  as a module.

2) Let  $L'$  be a quadratic lattice over  $\mathbf{Z}$  in some regular quadratic space  $U'$  over  $\mathbf{Q}$  satisfying  $dL' = dL$ ,  $\text{rank } L' = \text{rank } L$ ,  $t_p(L') \geq t_p(L)$  for any prime  $p$ . If there is an isometry  $\varphi$  from  $M$  to  $L'$  such that  $\varphi(M)$  is a direct summand of  $L'$  as a module, then  $L'$  is isometric to  $L$ .

*Proof.* Let  $\text{rank } L = 2$ ; by scaling we may assume that a matrix  $\begin{pmatrix} 2a' & b' \\ b' & 2c' \end{pmatrix}$  corresponding to  $L$  satisfies that  $a', b', c'$  are integers such that  $(a', b', c') = 1$ ,  $a' > 0$ . From the classical theory we know that there is an element  $u$  in  $L$  such that  $Q(u) = 2p$ , where  $p$  is a prime with  $(p, 2dL) = 1$ . Hence  $L$  has a matrix  $\begin{pmatrix} 2p & b \\ b & 2c \end{pmatrix}$  where  $0 < b < p$ . Let  $e$  be an integer such that  $e^2 \equiv -dL \pmod{p}$  and  $0 < e < p$ . From  $dL = 4pc - b^2$  follows  $b = e$  or  $p - e$ . If there is an integer  $x$  such that  $dL = 4px - e^2$ , then there is no integer  $y$  satisfying  $dL = 4py - (p - e)^2$ . Therefore the condition  $0 < b < p$  determines  $b$  uniquely. Now we put  $M = \mathbf{Z}[u]$ . If  $L'$  satisfies the condition 2), then  $L'$  has a matrix  $\begin{pmatrix} 2p & b'' \\ b'' & 2c'' \end{pmatrix}$  ( $b'', c'' \in \mathbf{Q}$ ), since  $L'$  contains a primitive vector  $u'$  with  $Q(u') = Q(u) = 2p$ .  $t_q(L') \geq t_q(L)$  implies  $b'', c'' \in \mathbf{Z}_q$  for any prime  $q$ . Hence  $b'', c''$  are integers, and we may assume  $0 < b'' < p$ . As above we have  $b'' = b$ . Hence  $L'$  is isometric to  $L$ . Let  $\text{rank } L$  be larger than 2. By scaling

we may assume that the scale of  $L$  is in  $\mathbf{Z}$ , and  $L$  is not negative definite. For brevity we denote  $\mathbf{Z}_p N$  by  $N_p$  for a quadratic lattice  $N$  over  $\mathbf{Z}$ . For a prime  $p$  dividing  $2dL$  we can take an element  $v_p$  in  $L_p$  such that  $v_p$  is in the orthogonal complement of a characteristic submodule of  $L_p$ . Put  $Q(v_p) = u_p p^{r_p}$ , where  $Q$  is the quadratic form associated with  $L$  and  $u_p$  is a unit of  $\mathbf{Z}_p$ , and  $r_p \geq 0$ . We take a prime  $q$  such that  $(q, 2dL) = 1$  and  $q \prod_{p|2dL} p^{r_p} \equiv Q(v_l) \pmod{l^t}$  for any prime  $l$  dividing  $2dL$  and a sufficiently large fixed integer  $t$ . Put  $a = q \prod_{p|2dL} p^{r_p}$ ; then  $Q(L_p)$  contains  $a$  for a prime  $p|2dL$ , since  $a^{-1}Q(v_p)$  is a square of a unit of  $\mathbf{Z}_p$ . If a prime  $p$  does not divide  $2dL$ , then  $L_p$  is unimodular and  $Q(L_p) = \mathbf{Z}_p$  (92:1b in [2]). Therefore from the non-negative-definiteness of  $L$  follows that  $U = QL$  represents  $a$  by virtue of the Minkowski-Hasse theorem. Since  $a^{-1}Q(v_p)$  is a square of unit of  $\mathbf{Z}_p$  for  $p$  dividing  $2dL$ , we may assume that  $Q(v_p) = a$  and the orthogonal complement of  $v_p$  in  $L_p$  is a characteristic submodule of  $L_p$ . We can take an element  $v$  in  $U$  such that  $Q(v) = a$ , and  $v$  and  $v_p$  are sufficiently near if  $p|2dL$ . Put  $S = \{p; v \notin L_p, \text{ and } \sigma_p v \in L_p \text{ for a rotation } \sigma_p \text{ with } \text{ord}_p \theta_p(\sigma_p) \equiv 1 \pmod{2}\}$ , where  $\theta_p$  stands for the spinor norm; then  $p \nmid 2dL$  if  $p \in S$ . We take a prime  $h \neq 2$  such that  $h \equiv \prod_{p \in S} p \pmod{(2dL)^t}$  and  $\left(\frac{-adL}{h}\right) = 1$ . Put  $u = \sigma(v)$ , where  $\sigma$  is a rotation of  $U$  whose spinor norm is  $h \prod_{p \in S} p$  (101:8 in [2]).

For a prime  $p$  with  $p \nmid 2hq dL$  there is a rotation  $\sigma_p$  such that  $\sigma_p \sigma^{-1} u = \sigma_p v \in L_p$  and  $\text{ord}_p \theta_p(\sigma_p) \equiv 0$  or  $1 \pmod{2}$  according to  $p \notin S$  or  $p \in S$  respectively, and then  $\text{ord}_p \theta_p(\sigma_p \sigma^{-1}) \equiv 0 \pmod{2}$ . Hence there is a rotation  $\eta_p$  such that  $\theta_p(\eta_p) = 1$ ,  $\eta_p(u) \in L_p$  by virtue of 92:5 in [2] for  $p \nmid 2hq dL$ . If  $p = h$ , then there is a rotation  $\eta_p$  such that  $\eta_p(u) \in L_p$  since  $Q(u) = a$  is a unit of  $\mathbf{Z}_p$  and  $L_p$  is unimodular. Since  $\eta_p(u)$  splits  $L_p$  and its orthogonal complement  $N_p$  in  $L_p$  is a unimodular lattice with  $\left(\frac{-dN_p}{h}\right) = \left(\frac{-adL}{h}\right) = 1$ ,  $N_p$  is isotropic. Hence we may assume that the spinor norm of  $\eta_p$  is 1 by virtue of 55:2a in [2]. For  $p|2dL$  put  $\eta_p = \sigma^{-1}$ ; then  $\eta_p(u)$  is sufficiently near to  $v_p$  and  $\theta_p(\eta_p) = 1$ . By the strong approximation theorem regarding the set  $\{p; \text{prime } \neq q\}$  as an indefinite set for  $U$ , there is a rotation  $\eta$  such that  $\eta$  and  $\eta_p$  are sufficiently near at both  $p$  dividing  $2dL$  and  $p$  satisfying  $u \notin L_p$  for  $p \nmid 2qdL$ , and  $\eta L_p =$

$L_p$  otherwise. Put  $\eta(w) = w$ ; then  $Q(w) = a$  and  $w \in L_p$  if  $p \neq q$ . Since  $\eta$  and  $\sigma^{-1}$  are sufficiently near for  $p|2dL$  and  $w = \eta\sigma(v)$  is sufficiently near to  $v_p$  for  $p|2dL$ , hence the orthogonal complement of  $w$  in  $L_p$  is a characteristic submodule in  $L_p$ . Moreover for  $p \nmid 2qdL$   $L_p$  is unimodular and  $Q(w)$  is a unit of  $\mathbf{Z}_p$ . This implies that the orthogonal complement of  $w$  is also a characteristic submodule in  $L_p$ . Put  $M = \{x \in L; x \perp w\}$ . Then a submodule  $M$  of  $L$  satisfies the condition 1) and  $dM = q^r m$ , where  $q$  is a prime with  $q \nmid 2dL$  and a prime  $p|2dL$  if  $p|m$ , and  $r \geq 0$ , and moreover  $M_p$  is a characteristic submodule of  $L_p$  for  $p \neq q$ . Let  $L'$  be a quadratic lattice in question in 2). Since  $L'$  represents  $M$  and  $dL' = dL$ ,  $U' = QL'$  is isometric to  $U = QL$ . Hence we may assume that  $L'$  is in  $U$  and  $L' \supset M$ . Since  $M_p$  is a characteristic submodule of  $L_p$  for  $p \neq q$ ,  $L'_p = L_p$  for  $p \neq q$ . Take a basis  $\{w_i\}$  of  $L_q$  such that  $M_q = \bigoplus_{i=1}^{n-1} \mathbf{Z}_q w_i$  ( $n = \text{rank } L$ ) and  $\text{ord}_q Q(w_1) \leq \dots \leq \text{ord}_q Q(w_{n-1})$ ; then a matrix corresponding to  $L_q$  is

$$\begin{pmatrix} a_1 q^{r_1} & & & b_1 \\ & \ddots & & \vdots \\ & & 0 & \\ 0 & & a_{n-1} q^{r_{n-1}} & b_{n-1} \\ b_1 \dots & & b_{n-1} & b_n \end{pmatrix},$$

where  $a_i$  is a unit of  $\mathbf{Z}_q$  and  $0 \leq r_1 \leq \dots \leq r_{n-1}$ . Since the determinant of this matrix is a unit of  $\mathbf{Z}_q$ , we see easily  $r_1 = \dots = r_{n-2} = 0$ . By taking  $w_n - \sum_{i=1}^{n-2} a_i^{-1} b_i w_i$  instead of  $w_n$ , we may assume that  $b_1 = \dots = b_{n-2} = 0$  in the matrix. Then  $N_q = \mathbf{Z}_q[w_{n-1}, w_n]$  is unimodular and  $-dN_q = b_{n-1}^2 - a_{n-1} b_n q^{r_{n-1}}$ . If  $r_{n-1} \geq 1$ , then  $b_{n-1}$  is a unit, and  $-dN_q$  is a square of a unit of  $\mathbf{Z}_q$ . If  $r_{n-1} = 0$ , then  $M_q$  is unimodular. Hence  $L_q$  has a basis  $z_1, \dots, z_n$  such that  $z_i \perp \mathbf{Z}_q[z_{n-1}, z_n]$  for  $i \leq n-2$ ,  $Q(z_{n-1}) = Q(z_n) = 0$ ,  $B(z_{n-1}, z_n) = 1$  and  $M_q = \mathbf{Z}_q[z_1, \dots, z_{n-2}, z_{n-1} + u_q q^r z_n]$ , where  $u_q$  is a unit. Since  $L'_q$  is unimodular and contains  $M_q$  primitively, we get  $L'_q = \mathbf{Z}_q[z_1, \dots, z_{n-2}] \perp K_q$ , where  $K_q$  is unimodular and  $z_{n-1} + u_q q^r z_n$  is primitive in  $K_q$ . Put  $K_q = \mathbf{Z}_q[z_{n-1} + u_q q^r z_n, cz_{n-1} + dz_n]$  ( $c, d \in \mathbf{Q}_q$ ); then  $Q(cz_{n-1} + dz_n) \in \mathbf{Z}_q$ ,  $B(z_{n-1} + u_q q^r z_n, cz_{n-1} + dz_n)$  is a unit, if  $r > 0$ . If  $r = 0$ , then  $c, d \in \mathbf{Z}_q$ . Hence we have  $K_q = \mathbf{Z}_q[z_{n-1}, z_n]$  or  $\mathbf{Z}_q[q^{-r} z_{n-1}, q^r z_n]$ . From  $w \perp M$  and  $(z_{n-1} - u_q q^r z_n) \perp M_q$  follows that two symmetries  $\tau_w, \tau_{z_{n-1} - u_q q^r z_n}$  are equal. Therefore we see  $\mathbf{Z}_q[q^{-r} z_{n-1}, q^r z_n] = \tau_w \mathbf{Z}_q[z_{n-1}, z_n]$ .

Thus we get  $L' = L$  or  $\tau_w L$  since  $L'_p = \tau_w L'_p = L_p$  for  $p \neq q$ , and  $L'_q = L_q$  or  $\tau_w L_q$ . This completes our proof.

For brevity we call  $M$  a characteristic submodule of  $L$ .

*Remark.* Our proof shows:

Let the scale of  $L$  be in  $\mathbf{Z}$  and  $\text{rank } L \geq 3$ ; if a direct summand  $M$  of  $L$  satisfies

1)  $M_p$  is a characteristic submodule of  $L_p$  if  $p|2dL$ ,

2)  $dM = q^r m$ , where  $q$  is a prime with  $q \nmid 2dL$ ,  $r \geq 0$  and  $p|2dL$  if a prime  $p$  divides  $m$ ,

then  $M$  is a characteristic submodule of  $L$ .

If we can take  $r = 0$  or  $1$ , then  $\varphi(M)$  is a direct summand of  $L'$  as a module in the assertion 2) if  $\varphi(M)$  is a submodule in  $L'$ . If  $\text{rank } L \neq 3$  and  $L$  is indefinite, then we can easily show to take  $r = 1$ . In definite cases analytic methods will be required.

**§2.** Let  $S, T$  be  $n \times n$  rational symmetric matrices. We say that  $S, T$  are equivalent if and only if there is an element  $U$  in  $GL(n, \mathbf{Z})$  such that  $S[U] = T$ . For a rational symmetric matrix  $S = (s_{ij})$  we define a quadratic lattice  $L = \mathbf{Z}[e_1, \dots, e_n]$  by  $B(e_i, e_j) = s_{ij}$ .  $L$  is called the quadratic lattice corresponding to  $S$ . Then  $dL = |S|$ .

**LEMMA.** Let  $S_i$  be positive definite rational matrices with  $|S_i| = d$  and  $\text{rank} = n$ , and suppose that they are not equivalent. Put  $\theta(\mathbf{Z}, S_i) = \sum e^{\pi i \text{tr}(S_i[G]Z)}$ , where  $G$  runs over  $M_{n, n-1}(\mathbf{Z})$ , and  $\mathbf{Z}^{(n-1)} = {}^t \mathbf{Z}$ ,  $\text{Im } \mathbf{Z} > 0$ ; then  $\theta(\mathbf{Z}, S_i)$  are linearly independent.

*Proof.* Obviously we may assume that  $S_i$  is integral. Denote by  $L_i$  the quadratic lattice corresponding to  $S_i$ ; then  $dL_i = d$ . Put  $\theta(\mathbf{Z}, S_i) = \sum a_i(T) e^{\pi i \text{tr}(TZ)}$ . For  $|T| \neq 0$ ,  $a_i(T)$  is the number of isometries from the quadratic lattice corresponding to  $T$  to  $L_i$ . Suppose that  $\theta(\mathbf{Z}, S_i)$  are linearly dependent and  $\sum c_i \theta(\mathbf{Z}, S_i) = 0$  with each  $c_i \neq 0$ . Let  $p_1, p_2, \dots, p_t$  be all primes dividing  $2d$ , and  $A_1$  be the set of  $L_i$  whose  $t_{p_1}(L_i)$  is minimal in the set  $\{t_{p_1}(L_i)\}$ . Inductively we define the set  $A_{k+1}$  as follows;  $A_{k+1}$  is the set of  $L_i$  whose  $t_{p_{k+1}}(L_i)$  is minimal in  $\{t_{p_{k+1}}(L_i); L_i \in A_k\}$ . For  $L_i$  in  $A_t$  we take a characteristic submodule  $M_i$  such that  $(M_i)_p$  is a characteristic submodule of  $(L_i)_p$  if  $p|2d$ , and  $dM_i = q_i^r m_i$ , where  $q_i$  is a prime with  $q_i \nmid 2d$ , and  $p|2d$  if a prime  $p$  divides  $m_i$  (Proof of

Theorem in § 1). Put  $r = \min_{\substack{L_i \in A_i \\ M_i}} r_i$ , and for some  $L_i$  in  $A_i$  and its characteristic submodule  $M_i$  we have  $dM_i = q_i^r m_i$ . If there is an isometry  $\sigma$  from  $M_i$  to  $L_j$ , then  $\sigma$  is extended to the isometry from  $QL_i$  to  $QL_j$ , and  $\sigma^{-1}(L_j)_{p_1} \supset (M_i)_{p_1}$ . By definition of a characteristic submodule we get  $\sigma^{-1}(L_j)_{p_1} = (L_i)_{p_1}$  and  $L_j$  is in  $A_1$ . Inductively we obtain  $\sigma^{-1}(L_j)_p = (L_i)_p$  for  $p|2d$  and  $L_j$  is in  $A_i$ . Suppose that  $\sigma(M_i)$  is not a direct summand of  $L_j$ ; then there is a direct summand  $N$  of  $L_j$  such that  $N \subseteq \sigma(M_i)$  and  $\text{rank } N = \text{rank } M_i$ . From  $\sigma^{-1}(L_j)_p = (L_i)_p$  for  $p|2d$  follows  $(M_i)_p \subset \sigma^{-1}(N)_p \subset (L_i)_p$ . Hence we have  $(M_i)_p = \sigma^{-1}(N)_p$  for  $p|2d$  since  $(M_i)_p$  is a direct summand of  $(L_i)_p$ , and  $dN = q_i^{r'} m_i$ ,  $r' \leq r - 2 < r$ . Hence  $N$  is a characteristic submodule of  $L_j$  if  $n \geq 3$  (Remark in § 1). This contradicts the minimality of  $r$ . In case of  $n = 2$ , from the classical theory we can take  $r_i = r = 1$ . Hence  $r' < 0$  is a contradiction. Therefore  $\sigma(M_i)$  is a direct summand of  $L_j$ . Hence  $L_j$  is isometric to  $L_i$  by virtue of Theorem in § 1. This means that we have  $a_i(T) \neq 0$  and  $a_j(T) = 0$  if  $j \neq i$  for the matrix corresponding to  $M_i$ . This contradicts  $c_i \neq 0$ .

*Remark 1.* Put  $\theta_p(Z, S_i) = \sum e^{\pi i \text{tr}(S_i[G]Z)}$ , where  $G$  runs over primitive matrices in  $M_{n, n-1}(Z)$ . The proof of Lemma states that  $\theta_p(Z, S_i)$  are linearly independent.

*Remark 2.* Let the class number of even integral positive definite quadratic forms over  $Z$  with  $\det = 1$ ,  $\text{rank} = 8k$  be  $h(8k)$ . Then we have  $h(8k)$  linearly independent Siegel modular forms with weight  $4k$ , degree  $8k - 1$  defined by  $\theta(Z, S_i)$  as above. The dimension of the space spanned by the corresponding Dirichlet series  $\sum_{\{T\} > 0} \frac{a(T)}{\varepsilon(T) |T|^s}$ , where  $a(T) = \#\{X \in M_{8k, 8k-1}(Z); S_i[X] = T\}$  and  $T$  runs over the representatives of equivalence classes of positive definite integral matrices, and  $\varepsilon(T) =$  the order of the group of units of  $T$ , is equal to the dimension of the space spanned by the Epstein zeta functions of  $S_i$  by Theorem 4 in p. 298 in [1] and it amounts to  $[k/3] + 1$ , since the space of elliptic modular forms with weight  $4k$  is spanned by theta functions, and its dimension is  $[k/3] + 1$ . Numerically we know  $h(8) = 1$ ,  $h(16) = 2$ ,  $h(24) = 24$ ,  $h(32) > 8 \cdot 10^8$ .

Let  $S = (s_{ij})$  be a positive definite real matrix with  $\text{rank} = n$ .  $L$  denotes a  $Z$ -lattice  $Z[e_1, \dots, e_n]$  which has an inner product defined by  $B(e_i, e_j) = s_{ij}$ . For a submodule  $M = Z[f_1, \dots, f_m]$  of  $L$  we denote  $\det(B(f_i, f_j))$  by  $dM$ . Denote by  $z_1, \dots, z_{n-1}$  a system of  $n - 1$  complex

variables and by  $s_1, \dots, s_n$  a system of  $n$  complex variables, the two being related by the equations

$$z_k = s_{k+1} - s_k + \frac{1}{2}, \quad k = 1, 2, \dots, n-1.$$

Now the Selberg's zeta function is defined by

$$\zeta^*(S; s_1, s_2, \dots, s_n) = \sum (dL_{n-1})^{-z_{n-1}} \cdot (dL_{n-2})^{-z_{n-2}} \dots (dL_1)^{-z_1},$$

where  $L_k$  runs over direct summands of  $L_{k+1}$  with  $\text{rank } L_k = k$  and  $L_n = L$ . This is absolutely convergent for  $\text{Re } z_k > 1$  ( $1 \leq k < n$ ) and satisfies certain functional equations (Theorem 1. p. 263 in [1]). Our aim in this section is to prove

**THEOREM.** *Let  $S_i$  be positive definite rational matrices with  $\text{rank} = n$ ,  $|S_i| = d$ . If they are not equivalent with each other, then  $\zeta^*(S_i; s_1, \dots, s_n)$  are linearly independent as functions of  $s_1, \dots, s_n$ . Especially the Selberg's zeta function is a complete analytic class invariant.*

*Proof.* Theorem is equivalent to the linear independence of  $\theta_p(\mathbf{Z}, S_i)$  by the Mellin transform in case of  $n = 2$  and it is true by virtue of Remark 1. Suppose that Theorem is true for  $n - 1$  but false for  $n$ ; then there are positive definite rational matrices  $S_i$  with  $\text{rank} = n$ ,  $|S_i| = d'$  such that

$$\sum a_i \zeta^*(S_i; s_1, \dots, s_n) = 0,$$

where  $S_i$  are not equivalent with each other. Put

$$u(Y) = u_{1,2,\dots,n-2}(Y) = |Y|^{\sum_{k=1}^{n-2} kz_k/(n-1)} \sum_U \prod_{k=1}^{n-2} |Y[U]_k|^{-z_k},$$

where  $Y$  is positive definite and of  $\text{rank} = n - 1$ ,  $U$  runs over the factor

set  $GL(n-1, \mathbf{Z}) / \left\{ \begin{pmatrix} * & * \\ \cdot & \cdot \\ 0 & * \end{pmatrix} \in GL(n-1, \mathbf{Z}) \right\}$ ,  $Y = \begin{pmatrix} \overline{Y}^k & * \\ * & * \end{pmatrix}$  and  $z_k = s_{k+1}$

$- s_k + \frac{1}{2}$ . This is a Größen-character in the sense of §10 in [1]. We define a function  $R_i(s)$  by

$$R_i(s) = \int_F \theta_p(iY, S_i) |Y|^s u(Y^{-1}) dv,$$

where  $F$  is the Minkowski's domain of reduced matrices in the space



of all positive definite matrices with rank =  $n - 1$  and  $dv = |Y|^{-n/2} \prod_{s \leq t} dy_{st}$ .

Putting

$$\begin{aligned} \theta_p(iY, S_i) &= \sum_{T > 0} a_i(T) e^{-2\pi \operatorname{tr}(TY)}, \\ R_i(s) &= \int_{\mathbb{F}} \sum_{T > 0} a_i(T) e^{-2\pi \operatorname{tr}(TY)} |Y|^s u(Y^{-1}) dv \\ &= \sum \frac{a_i(T)}{\varepsilon(T)} \int_{Y^{(n-1)} > 0} e^{-2\pi \operatorname{tr}(TY)} |Y|^s u(Y^{-1}) dv, \end{aligned}$$

where  $T$  runs over representatives of equivalence classes of positive definite rational matrices of rank =  $n - 1$ ,

$$= \pi^{(n-1)(n-2)/4} (2\pi)^{(1-n)s} \prod_{k=1}^{n-1} \Gamma(s - c_k) \sum \frac{a_i(T)}{\varepsilon(T)} |T|^{-s} u(T),$$

where  $c_k$  is a certain complex number (p. 94 in [1]), thus we get

$$R_i(s) = \pi^{(n-1)(n-2)/4} (2\pi)^{(1-n)s} \prod_{k=1}^{n-1} \Gamma(s - c_k) \zeta^*(S_i; s'_1, \dots, s'_n),$$

where  $s'_i$  is defined by

$$z_k = s'_{k+1} - s'_k + \frac{1}{2} \quad (k < n - 1), \quad -s + \sum_{k=1}^{n-2} k z_k / (n - 1) = s'_n - s'_{n-1} + \frac{1}{2}.$$

Hence our assumption implies  $\sum a_i R_i(s) = 0$ . On the other hand, from Remark 1 follows that  $\sum a_i \theta_p(iY, S_i) = \sum a(T) e^{-2\pi \operatorname{tr}(TY)}$  is not zero. This yields that there is a  $T_0$  such that  $a(T_0) \neq 0$ . Regarding  $\sum a_i R_i(s)$  as Dirichlet series with respect to  $s$ , we obtain

$$\sum \frac{a(T)}{\varepsilon(T)} u(T) = 0,$$

where  $T$  runs over representatives of classes with  $|T| = |T_0|$ . This contradicts our assumption since  $|T|^{-\sum_{k=1}^{n-2} k z_k / (n-1)} u(T)$  is by definition the Selberg's zeta function of positive definite matrix  $T^{(n-1)}$ .

**COROLLARY.** Let  $f(Z) = \sum a(T) e^{2\pi i \operatorname{tr}(TZ)}$  be a Siegel modular form of degree  $n$ . If the corresponding Dirichlet series

$$\sum_{\{T\} > 0} \frac{a(T) u(T)}{\varepsilon(T) |T|^s}$$

with a Größen-character  $u(T)$  as  $|T|^{k \sum_{j=1}^{n-1} s_j/n} \zeta^*(T; s_1, s_2, \dots, s_n)$  is zero as a function of  $s, s, \dots, s_n$ , then  $a(T) = 0$  for  $T > 0$ .

## REFERENCES

- [ 1 ] H. Maaß, Siegel's modular forms and Dirichlet series, Lecture Notes in Math. 216, Springer-Verlag, 1971.
- [ 2 ] O. T. O'Meara, Introduction to quadratic forms, Springer-Verlag, 1963.

*Nagoya University*