Pacific Journal of Mathematics

SPINOR NORMS OF LOCAL INTEGRAL ROTATIONS. II

ANDREW GEORGE EARNEST AND JOHN SOLLION HSIA

Vol. 61, No. 1 November 1975

PACIFIC JOURNAL OF MATHEMATICS
Vol. 61, No. 1, 1975

SPINOR NORMS OF LOCAL INTEGRAL ROTATIONS, II

A. G. EARNEST AND J. S. HSIA

Dedicated to Professor Olga Taussky Todd's Birthday

The spinor norms of integral rotations on an arbitrary quadratic form over a dyadic local field in which 2 is prime are determined. Results are stated in terms of the components of a Jordan splitting of the given form. Results obtained are applied to improve a theorem of Kneser giving sufficient conditions for an indefinite Z-lattice to have class number 1.

The behavior of integral quadratic forms over a global field can be partially described in terms of the local behavior relative to each of the prime spots on the field. In particular, in computing the number of spinor genera in the genus of a given form, it is necessary to compute the spinor norm of the group of local integral rotations at each prime spot (see e.g. [3], [4]). These computations have been performed whenever the local form is modular (see [2]). In the case of an arbitrary form, the Jordan splitting can be used to decompose the given form as an orthogonal sum of modular forms. In the present article we deal with the problem of obtaining the desired spinor norm by using these modular components. When the spot in question is nondyadic, this problem has been solved by Kneser in [3]. We handle the case of a dyadic spot in which 2 is prime. The significance of the restriction of 2 being prime is that strong use is made of theorems on the generation of the local integral orthogonal groups in this case (see [5]) which are not known for arbitrary dyadic local fields.

We adopt the notation of [4]. So we will consider a lattice L over a dyadic local field F in which 2 is prime. Denote the integers and units in F by $\mathfrak{o}$ and $\mathfrak{U}$, respectively; $\Delta = 1 + 4\rho$ denotes a nonsquare unit of quadratic defect $4\mathfrak{o}$. To emphasize the distinction between spaces over F and lattices over $\mathfrak{o}$, we will use $[\alpha_1, \cdots, \alpha_n]$ to denote spaces and $\langle\alpha_1, \cdots, \alpha_n\rangle$ to denote lattices. $(\,,\,)$ will denote the Hilbert symbol on F and θ the spinor norm function.

For any lattice L, the Jordan decomposition of L can be obtained as in [4]. We determine $\theta(0^+(L))$, where $0^+(L)$ denotes the group of rotations of L, in terms of invariants of the Jordan components. The paper is divided into 4 sections. In the first we perform the calculations for the binary case. The second and third deal with the various possible types of Jordan decompositions and the fourth section shows an application of these calculations to improve the bounds obtained in a theorem of Kneser [3, Satz 5] giving sufficient conditions for an indefinite $\boldsymbol{Z}$-lattice to have class number 1. Furthermore, the new bounds obtained are shown to be the best possible.

The calculations which appear in this paper will be further applied in a subsequent paper investigating the behavior of the spinor genus of an integral quadratic form over a global field under an extension of the field of coefficients.

I. **Binary case.** We begin by computing $\theta(0^+(L))$ where $\dim L=2$. These binary lattices are the fundamental building blocks on which higher dimensional computations will be based.

If L is modular then $\theta(0^+(L))$ has been determined in [2]. So we deal only with the nonmodular case. Since the spinor norm is not affected by scaling, we may assume that L represents 1. Thus, for the remainder of this section we deal with

$$L \cong \langle 1\rangle \perp \langle 2^r\alpha\rangle,\ r \geqq 1,\ \alpha \in \mathfrak{U} \longleftrightarrow \mathfrak{o}x + \mathfrak{o}y$$

We introduce some notation that will be used throughout: For any lattice L $P(L) = \{v \in L\colon v \text{ maximal and } S_v \in 0(L)\}$ and $D(L) = Q(P(L))$. The problem can now be reduced as follows: Any $\sigma \in 0^+(L)$ can be expressed as a product of 2 symmetries of FL, say $\sigma = S_u S_v$, where S_u can be chosen arbitrarily. In particular, choose $u = x$ so $S_v = S_x\sigma \in 0(L)$ and $\theta(\sigma) = \theta(S_v) = Q(v)\dot{F}^2$. Thus, $\theta(0^+(L)) = D(L)\dot{F}^2$. So in the present case, it suffices to determine $D(L)$.

First, we characterize $P(L)$:

LEMMA 1.1. *Consider* $v = Ax + By \in L$, $A, B \in \mathfrak{o}$

(i) *If* $A \in \mathfrak{U}$, *then* $v \in P(L)$

(ii) *If* $A \notin \mathfrak{U}$, *and* $r \geqq 3$, *then* $v \in P(L) \Leftrightarrow B \in \mathfrak{U}$ *and either* $\operatorname{ord} A = 1$ *or* $\operatorname{ord} A \geqq r-1$

Proof of (ii)

(1) Suppose $\operatorname{ord} A = 1$

Then $B(v, L) = B(v, x)\mathfrak{o} = A\mathfrak{o}$ and $Q(v) = A^2 + 2^r B^2\alpha$.

So $2B(v, L) = 2A\mathfrak{o} = A^2\mathfrak{o} = Q(v)\mathfrak{o}$

$$\frac{2B(v, L)}{Q(v)} \subseteqq \mathfrak{o} \Leftrightarrow S_v \in 0(L).$$

(2) Suppose $\operatorname{ord} A \geqq r-1$.

Then

$$B(v, L) \subseteqq \begin{cases} A\mathfrak{o} \text{ if } \operatorname{ord} A = r-1 \\ 2^r\mathfrak{o} \text{ if } \operatorname{ord} A > r-1 \end{cases} \subseteqq 2^{r-1}\mathfrak{o}\,.$$

Ord $Q(v) = \operatorname{ord}(A^2 + 2^r B^2\alpha) = r$ since $\operatorname{ord} A^2 \geqq (r-1)^1 > r$.

So $2B(v, L) \subseteqq 2^r\mathfrak{o} = Q(v)\mathfrak{o}$ and, thus, $S_v \in O(L)$.

(3) Suppose $1 \lneqq \operatorname{ord} A \lneqq r-1$.
Then $B(v, L) = B(v, x)\mathfrak{o} = A\mathfrak{o}$ since $\operatorname{ord} A \lneqq r-1$.

$$\operatorname{Ord} Q(v) = \operatorname{ord}(A^2 + 2^r B^2 \alpha)\begin{cases} \geqq \operatorname{ord} A^2 & \text{if } \operatorname{ord} A^2 \leqq r \\ = r & \text{if } \operatorname{ord} A^2 > r\,. \end{cases}$$

In either case, $2A\mathfrak{o} \nsubseteq Q(v)\mathfrak{o}$. Thus, $S_v \notin O(L)$.

So if $r \geqq 3$, the set $P(L)$ can be decomposed as $P(L) = P_1(L) \cup P_2(L)$ where

$$P_1(L) = \{v = Ax + By\colon \operatorname{ord} A = 1 \text{ or } 0\}$$
$$P_2(L) = \{v = Ax + By\colon \operatorname{ord} B = 0 \text{ and } \operatorname{ord} A \geqq r-1\}\,.$$

We now determine $Q(P_2(L))$ when $r \geqq 3$.

LEMMA 1.2. *Let* $r \geqq 3$. *Then* $Q(P_2(L)) = 2^r[Q(K) \cap \mathfrak{U}]\dot{F}^2$ *where* $K \cong \langle \alpha, 2^{r-2}\rangle$.

Proof. Let $v \in P_2(L)$ where $v = Ax + By$ and $t = \operatorname{ord} A \geqq r-1$. So

$$Q(v) = A^2 + 2^r B^2\alpha = 2^{2t}A_0^2 + 2^r B^2 \alpha \text{ where } A = 2^t A_0,\ A_0 \in \mathfrak{U}$$
$$= 2^r[2^{2t-r}A_0^2 + B^2\alpha] = 2^r[2^{r-2}(2^{2t-2r+2}A_0^2) + B^2\alpha]\,.$$

Let $u = 2^{t-r+1}A_0 y' + Bx'$ where $K = \mathfrak{o}x' + \mathfrak{o}y'$. Then $Q(v) = 2^r Q(u)$ and $Q(u) \in Q(K) \cap \mathfrak{U}$.

Conversely, let $\xi = 2^{r-2}C^2 + \alpha D^2 \in Q(K) \cap \mathfrak{U}$. Write $C = 2^c C_0$ where $C_0 \in \mathfrak{U}$. Then $\xi = 2^{r-2+2c}C_0^2 + \alpha D^2$, $C_0 \in \mathfrak{U}$, $D \in \mathfrak{U}$. So $2^r\xi = 2^{2r+2c-2}C_0^2 + 2^r\alpha D^2 = (2^{r+c-1}C_0)^2 + 2^r\alpha D^2$. Letting $v = 2^{r+c-1}C_0 x + Dy$, we obtain $v \in P_2(L)$ since $c \geqq 0$ and, furthermore, $Q(v) \in 2^r\xi\dot{F}^2$.

PROPOSITION 1.3. *Let* $r \geqq 5$. *Then* $\theta(0^+(L)) = \dot{F}^2 \cup 2^r\alpha\dot{F}^2$.

Proof. Follows from 1.2 and the Local Square Theorem.

PROPOSITION 1.4. *Let* $r = 1$. *Then*
(1) $Q(L) \cap \mathfrak{U} = Q(FL) \cap \mathfrak{U}$.
(2) $\theta(0^+(L)) = Q(FL)\dot{F}^2$.

Proof. Suppose that $\gamma \in Q(FL) \cap \mathfrak{U}$, say $\gamma = A^2 + 2\alpha B^2$, with $A, B \in \dot{F}$. By the Principle of Domination $0 = \operatorname{ord}\gamma = \min\{\operatorname{ord} A^2, \operatorname{ord} 2\alpha B^2\}$; so $A \in \mathfrak{U}$ and $B \in \mathfrak{o}$. Hence, $\gamma \in Q(L) \cap \mathfrak{U}$.

To prove (2), note that if $\tau \in Q(FL)$, there is some $\mu \in F$ so that ord $\tau\mu^2 = 0$ or 1. As above, the Principle of Domination gives $Q(L) \cap 2\mathfrak{u} = Q(FL) \cap 2\mathfrak{u}$. In particular, $\tau\mu^2 \in Q(L)$, say $\tau\mu^2 = Q(v)$, $v \in L$. Furthermore, $v \in P(L)$ since ord $Q(v) = 0$ or 1. On the other hand, it is clear that $\theta(0^+(L)) = D(L)\dot{F}^2 \subseteq Q(FL)\dot{F}^2$, and equality follows.

LEMMA 1.5. *Let $r = 2$. Then* $(Q(L) \cap \mathfrak{U})\dot{F}^2 = \dot{F}^2 \cup \varDelta\dot{F}^2$.

Proof. Suppose $\gamma \in Q(L) \cap \mathfrak{U}$; say $\gamma = A^2 + 4B^2\alpha$ with $A \in \mathfrak{U}$. So $\gamma = A^2 + 4B^2\alpha = A^2(1 + 4(B/A)^2\alpha) = A^2\gamma'$ where $\gamma' \in \mathfrak{U}$ and the quadratic defect of $\gamma' \subseteq 4\mathfrak{o}$. Thus, $\gamma' \in \dot{F}^2$ or $\gamma' \in \varDelta\dot{F}^2$ and the same is true for γ.

Conversely, we need to verify that $\varDelta \in Q(L)$. Consider the lattices $L = \langle 1, 4\alpha\rangle$ and $K = \langle \varDelta, 4\alpha\varDelta^{-1}\rangle$. By a computation of Hilbert symbols, it follows that $FL \cong FK$. It now follows from 93:29 [4] that $L \cong K$. So $\varDelta \in Q(L)$ as desired.

PROPOSITION 1.6. *Let $r = 2$. Then* $\theta(0^+(L)) = (Q(FL) \cap \mathfrak{U})\dot{F}^2$.

Proof. We first show that $D(L) \subseteq \mathfrak{U}\dot{F}^2$. Let $v \in P(L)$, say $v = Ax + By$. Clearly, $A \in \mathfrak{U} \Rightarrow Q(v) \in \mathfrak{U}$. So consider $A \in 2\mathfrak{o}$ and $B \in \mathfrak{U}$; write $A = 2^tA_0$, with $t \geqq 1$, $A_0 \in \mathfrak{U}$. If $t > 1$, then $Q(v) = 2^{2t}A_0^2 + 4\alpha B^2 \in 4\mathfrak{U}$. If $t = 1$, $Q(v) = 4(A_0^2 + \alpha B^2)$. So

$$B(v, L) = B(v, x)\mathfrak{o} = 2A_0\mathfrak{o} .$$

Then $S_v \in 0(L) \Rightarrow 2B(v, L) = 4\mathfrak{o} \subseteq Q(v)\mathfrak{o} \Rightarrow Q(v) \in 4\mathfrak{U}$. Thus, $D(L) \subseteq (Q(FL) \cap \mathfrak{U})\dot{F}^2$.

Conversely, suppose that $\zeta \in Q(FL) \cap \mathfrak{U}$. In that case, $[\zeta, \zeta^{-1}\alpha] \cong [1, \alpha]$. Consider the corresponding lattices $K = \langle\zeta, \zeta^{-1}\alpha\rangle$ and $L' = \langle 1, \alpha\rangle$. Since K and L' are both proper unimodular lattices on the same space, it follows from 93:16 of [4] that $K \cong L'$. So $\zeta \in Q\langle 1, \alpha\rangle$, say $\zeta = A^2 + \alpha B^2$ with $A, B \in \mathfrak{o}$. We consider several possibilities:

(i) Suppose $A, B \in \mathfrak{U}$. Then let $v = 2Ax + By$.

$$Q(v) = 4A^2 + 4\alpha B^2 = 4(A^2 + \alpha B^2) = 4\zeta$$

So $Q(v) \in \zeta\dot{F}^2$ and $v \in P(L)$ since $\zeta \in \mathfrak{U}$.

(ii) Suppose $A \in \mathfrak{U}$, $B \in 2\mathfrak{o}$; write $B = 2^tB_0$ with $B_0 \in \mathfrak{U}$, $t \geqq 1$. Let $v = Ax + 2^{t-1}B_0y$. Then

$$Q(v) = A^2 + 4\alpha(2^{2t-2}B_0^2) = A^2 + 2^{2t}B_0^2\alpha = A^2 + \alpha B^2 = \zeta$$

(iii) Suppose $A \in 2\mathfrak{o}$, $B \in \mathfrak{U}$; write $A = 2^tA_0$ with $t \geqq 1$, $A_0 \in \mathfrak{U}$. Let $v = 2^{t+1}A_0x + By$. Then

$$Q(v) = 2^{2t+2}A_0^2 + 4\alpha B^2 = 4(2^{2t}A_0^2 + \alpha B^2) = 4\zeta .$$

So in any case, we have found a vector $v \in P(L)$ such that $Q(v) \in \zeta \dot{F}^2$.

PROPOSITION 1.7. *Let* $r = 3$. *Then* $\theta(0^+(L)) = Q(FL)\dot{F}^2$.

Proof. Consider $v \in P(L)$, $v = Ax + By$. If $v \in P_1(L)$, then $A \in \mathfrak{U}$ or $A \in 2\mathfrak{U}$. $A \in \mathfrak{U} \Rightarrow Q(v) \in A^2\dot{F}^2 = \dot{F}^2$. $A \in 2\mathfrak{U} \Rightarrow Q(v) = 4(A_0^2 + 2\alpha B^2) \in Q\langle 1, 2\alpha\rangle \cap \mathfrak{U})\dot{F}^2$. On the other hand, $(Q\langle 1, 2\alpha\rangle \cap \mathfrak{U}) \subseteqq Q(P_1(L))$. Using 1.4, $Q(P_1(L))\dot{F}^2 = (Q[1, 2\alpha] \cap \mathfrak{U})\dot{F}^2$.

If $v \in P_2(L)$, then by 1.2, $Q(P_2(L))\dot{F}^2 = 8(Q(K) \cap \mathfrak{U})\dot{F}^2$ where $K = \langle \alpha, 2\rangle$. So

$$\begin{aligned} Q(P_2(L))\dot{F}^2 &= 2(Q[\alpha, 2] \cap \mathfrak{U})\dot{F}^2 = (Q[2\alpha, 4] \cap 2\mathfrak{U})\dot{F}^2 \\ &= Q[1, 2\alpha] \cap 2\mathfrak{U})\dot{F}^2 . \end{aligned}$$

PROPOSITION 1.8. *Let* $r = 4$. *Then*

$$\theta(0^+(L)) = \dot{F}^2 \cup \alpha\dot{F}^2 \cup \Delta\dot{F}^2 \cup \alpha\Delta\dot{F}^2 .$$

Proof. $Q(P_2(L)) = 16(Q\langle \alpha, 4\rangle \cap \mathfrak{U})\dot{F}^2$ by 1.2. By 1.5, $(Q\langle \alpha, 4\rangle \cap \mathfrak{U})\dot{F}^2 = \alpha\dot{F}^2 \cup \alpha\Delta\dot{F}^2$. Also by 1.5, $Q(P_1(L)) = \dot{F}^2 \cup \Delta\dot{F}^2$ and the result follows.

1.9. The results of this section can now be summarized as follows:

$$\theta(0^+(L)) = \begin{cases} \{\gamma \in \dot{F}: (\gamma, -2\alpha) = +1\} & \text{if } r = 1, 3 \\ \{\gamma \in \mathfrak{U}\dot{F}^2: (\gamma, -\alpha) = +1\} & \text{if } r = 2 \\ \dot{F}^2 \cup \alpha\dot{F}^2 \cup \Delta\dot{F}^2 \cup \alpha\Delta\dot{F}^2 & \text{if } r = 4 \\ \dot{F}^2 \cup 2^r\alpha\dot{F}^2 & \text{if } r \geqq 5 . \end{cases}$$

II. Higher dimensional cases—1-dimensional components. In this section, let L be a lattice of dim $\geqq 3$ with Jordan splitting

$$L = \langle 1\rangle \perp \langle 2^{r_2}\alpha_2\rangle \perp \cdots \perp \langle 2^{r_n}\alpha_n\rangle$$

where $r_i \in \boldsymbol{Z}$ and $\alpha_i \in \mathfrak{U}$, $i = 1, \cdots, n$, and $r_i < r_{i+1}$ for $i = 1, \cdots, n-1$, $r_1 = 0$.

In this section we make strong use of a theorem of O'Meara and Pollak which states that whenever $F \neq \boldsymbol{Q}_2$, the group $O(L)$ is generated by symmetries of L. In order to compute $\theta(0^+(L))$ it therefore suffices to compute $Q(P(L))$. In case $F = \boldsymbol{Q}_2$, $O(L)$ can be generated by symmetries of L along with the Eichler transformations E_w^i. But it is known (see [1]) that $\theta(E_w^i) = 1$. Thus the problem of computing $\theta(0^+(L))$ can again be reduced to that of finding $Q(P(L))$.

Theorem 2.2 gives sufficient conditions for $\theta(0^+(L)) = \dot{F}$. Then the problem of computing $Q(P(L))$ is essentially reduced to the same problem for certain binary sublattices, with the result appearing as 2.7.

NOTATION 2.1. Let $L = \langle 1\rangle \perp \langle 2^{r_2}\alpha_2\rangle \perp \cdots \perp \langle 2^{r_n}\alpha_n\rangle$. Then for $j = 1, \cdots, n-1$

$$\begin{aligned} L_{j,j+1} &= \langle 2^{r_j}\alpha_j\rangle \perp \langle 2^{r_{j+1}}\alpha_{j+1}\rangle \\ \xi_j &= 2^{r_{j+1}-r_j}\alpha_{j+1}\alpha_j^{-1} \\ r(L_{j,j+1}) &= r_{j+1} - r_j \\ I_{j,j+1} &= (\dot{F}/\dot{F}^2\colon \theta(0^+L_{j,j+1}))) \,. \end{aligned}$$

THEOREM 2.2. *Suppose there is at least one k for which $r(L_{k.k+1}) = 1$ or 3. Then if $r_s - r_t = 2$ or 4 for any $s, t = 1, \cdots, n$, we have $\theta(0^+(L)) = \dot{F}$.*

Proof. By 1.9, $\theta(0^+(L_{k,k+1}))$ has index 2 in $\dot{F}$ and does not contain the coset $\Delta\dot{F}^2$. On the other hand, 1.9 also yields $\Delta \in \theta(0^+(L'))$ where $L' = \langle 2^{r_s}\alpha_s\rangle \perp \langle 2^{r_t}\alpha_t\rangle$. Hence, $\theta(0^+(L)) = \dot{F}$.

We now wish to examine those lattices which do not satisfy the conditions of 2.2. It is convenient to regroup the Jordan components to obtain perhaps larger sublattices. The role of these sublattices is made clear by 2.4.

NOTATION 2.3. Let $\hat{L}_1 = \langle 1, 2^{r_2}\alpha_2, \cdots, 2^{r_{s_1}}\alpha_{s_1}\rangle$ where s_1 is taken to be the largest integer for which $r_{j+1} - r_j \leqq 4$ for all $j = 1, \cdots, s_1 - 1$ (in particular, $L_1 = \langle 1\rangle \Leftrightarrow r(L_{1,2}) \geqq 5$). $\hat{L}_2, \cdots, \hat{L}_t$, are defined inductively as follows: if $\hat{L}_k = \langle 2^{r_p}\alpha_p, \cdots, 2^{r_q}\alpha_q\rangle$ where $q = p + s_k$, then $\hat{L}_{k+1} = \langle 2^{r_{q+1}}\alpha_{q+1}, \cdots, 2^{r_{q+s_{k+1}}}\alpha_{s_{k+1}}\rangle$ where s_{k+1} is taken to be the larger integer for which $r_{q+j+1} - r_{q+1} \leqq 4$ for all $j = 1, \cdots, s_{k+1} - 1$. Thus, we obtain a new (generally non-Jordan) splitting

$$L = \hat{L}_1 \perp \cdots \perp \hat{L}_{t'} \,.$$

PROPOSITION 2.4. *Let $v \in P(L)$. Then $Q(v) \in Q(v')\dot{F}^2$ where $v' \in P(\hat{L}_s)$ for some $s = 1, \cdots, t'$.*

Proof. Write $v = \sum_{j=1}^n A_j x_j$ where $A_j \in \mathfrak{o}$ and $Q(x_j) = 2^{r_j}\alpha_j$. Let k be the largest integer for which ord $(2^{r_k}A_k^2)$ is minimal. Let m be the largest integer for which $m < k$ and $r_k - r_m \geqq 5$, and let h be the smallest integer for which $k < h$ and $r_h - r_k \geqq 5$. Define $v' = \sum_{j=m+1}^{h-1} A_j x_j$.

We first verify that $Q(v) \in Q(v')\dot{F}^2$. $S_v \in 0(L)$ forces $\operatorname{ord} A_k \leqq 1$ and $\operatorname{ord} Q(v') = r_k$. In particular, if $s \geqq h$ we have

$$r_s \geqq r_h \geqq \operatorname{ord} Q(v') + 3 .$$

So by the Local Square Theorem, $Q(v') + A_s^2 2^{r_s}\alpha_s \in Q(v')\dot{F}^2$. On the other hand, if $j < k$, then $S_v \in 0(L) \Rightarrow \operatorname{ord}(2^{r_j+1}A_j) \geqq \operatorname{ord}(A_k^2 2^{r_k}) \Rightarrow \operatorname{ord} A_j + r_j + 1 \geqq 2 \operatorname{ord} A_k + r_k \Rightarrow \operatorname{ord} A_j \geqq 2 \operatorname{ord} A_k + (r_k - r_j - 1)$. So $\operatorname{ord}(2^{r_j}A_j^2) \geqq 2 \operatorname{ord} A_k + 2(r_k - r_j - 1) + r_j = 2 \operatorname{ord} A_k + 2r_k - r_j - 2 = \operatorname{ord}(A_k^2 2^{r_k}) + (r_k - r_j - 2)$. In particular, whenever $u \leqq m$, we get $\operatorname{ord}(2^{r_u}A_u^2) \geqq \operatorname{ord}(A_k^2 2^{r_k}) + 3 = \operatorname{ord} Q(v') + 3$. So that again $Q(v') + A_u^2 2^{r_u}\alpha_u \in Q(v')\dot{F}^2$. It now follows that $Q(v) \in Q(v')\dot{F}^2$. By the choice of m and h, $v' \in \hat{L}_s$ for some s.

Finally, if $A_j \in \mathfrak{U}$ for some $j, m+1 \leqq h-1$, then $v' \in P(\hat{L}_s)$. On the other hand, if $A_j \in 2\mathfrak{o}$ for all such j, consider $v'' = v'/2 \in \hat{L}_s$. In particular, $A_k \in 2\mathfrak{U}$, so $v'' \in P(\hat{L}_s)$ and $Q'(v') \in Q(v'')\dot{F}^2$.

PROPOSITION 2.5. *Let $L \cong \langle 1, 2^{r_2}\alpha_2, \cdots, 2^{r_n}\alpha_n\rangle$ with r_i even for all $i = 2, \cdots, n$. Given $v \in P(L)$, there exists $v' \in P(L_{j,j+1})$ for some $j, 1 \leqq j \leqq n-1$, so that $Q(v) \in Q(v')\dot{F}^2$.*

Proof. Write $v = \sum_{i=1}^n A_i x_i$. Let k be the largest integer for which $\operatorname{ord}(2^{r_k}A_k^2)$ is minimal.

(1) Suppose there exists $j \neq k$ for which $\operatorname{ord}(2^{r_j}A_j^2) = \operatorname{ord}(2^{r_k}A_k^2)$. Since $S_v \in 0(L)$, it follows that $k = j+1$ and $r_k = r_j + 2$; furthermore, $A_k \in \mathfrak{U}$ and $\operatorname{ord} Q(v) = r_k$. If $h \neq j, k$ then

$$\operatorname{ord}(2^{r_h}A_h^2) \geqq \operatorname{ord} Q(v) + 2$$

since r_h is even. Thus $Q(v)/Q(A_j x_i + A_{j+1}x_{j+1}) \equiv 1 \pmod{4\mathfrak{o}}$.

Consider the vector $\tilde{v} = A_j x_j + A_{j+1}x_{j+1}$. Then $2B(\tilde{v}, L_{j,j+1}) \subseteqq 2B(v, L) \subseteqq Q(v)\mathfrak{o} = Q(\tilde{v})\mathfrak{o}$ and thus $\tilde{v} \in P(L_{j,j+1})$. Furthermore,

$$Q(P(L_{j,j+1})) = 2^{r_j}\alpha_j\{\gamma \in \mathfrak{U}\dot{F}: (\gamma, -\xi_j) = +1\}$$

by 1.6. Thus, $Q(\tilde{v}) = 2^{r_j+2}\alpha_j\tilde{\varepsilon}$ with $\tilde{\varepsilon} \in \mathfrak{U}$ and $(\tilde{\varepsilon}, -\xi_j) = +1$. Write $Q(v) = 2^{r_j+2}\alpha_j\varepsilon$ with $\varepsilon \in \mathfrak{U}$; then $\varepsilon \equiv \tilde{\varepsilon} \pmod{4\mathfrak{o}}$ since $Q(v)/Q(\tilde{v}) \equiv 1 \pmod{4\mathfrak{o}}$. Hence, $(\varepsilon, -\xi_j) = +1$ and $Q(v) \in Q(P(L_{j,j+1}))\dot{F}^2$.

(2) So now assume that $\operatorname{ord}(2^{r_j}A_j^2) \geqq \operatorname{ord}(2^{r_k}A_k^2) + 2$ for all $j \neq k$. Thus, $Q(v)/2^{r_k}\alpha_k A_k^2 \equiv 1 \pmod{4\mathfrak{o}}$. Note that $S_v \in 0(L)$ forces $\operatorname{ord} A_j \leqq 1$. Now if both $r_k - r_{k-1} \geqq 6$ and $r_{k+1} - r_k \geqq 6$, by the

Local Square Theorem $Q(v) \in 2^{r_k} A_k^2 \alpha_k \mathfrak{U}^2$. In particular, $Q(v) \in Q(P(L_{k,k+1}))\dot{F}^2$. Otherwise, one of $r_k - r_{k-1}$ and $r_{k+1} - r_k$ is $\leqq 4$; let us say that $r_{k+1} - r_k \leqq 4$. Then $Q(v) \in 2^{r_k} A_k^2 \alpha_k \dot{F}^2 \cup 2^{r_k} A_k^2 \alpha_k \Delta \dot{F}^2 \subseteqq Q(P(L_{k,k+1}))\dot{F}^2$ by 1.6 and 1.8.

PROPOSITION 2.6. *Let $L \cong \langle 1, 2^{r_2}\alpha_2, \cdots, 2^{r_n}\alpha_n \rangle$ with r_i a multiple of* 3 *for each $i = 2, \cdots, n$. Given $v \in P(L)$, there exists $v' \in P(L_{j,j+1})$ for some j, $1 \leqq j \leqq n-1$, so that $Q(v) \in Q(v')\dot{F}^2$.*

Proof. The proof is analogous to proof of 2.5. Using the notation of that proof, if $A_k \in \mathfrak{U}$, then $Q(v) \in Q(P(L_{k-1,k}))\dot{F}^2$; if $A_k \in 2\mathfrak{U}$, then $Q(v) \in Q(P(L_{k,k+1}))\dot{F}^2$. When $S_v \in 0(L)$, these exhaust all possibilities.

THEOREM 2.7. *Suppose that L does not satisfy the hypotheses of* 2.2. *Then*

$$\theta(0^+(L)) = \left\{ \prod_{i=1}^{\text{even}} Q(v_i) \colon v_i \in P(L_{j_i, j_i+1}),\ 1 \leqq j_i \leqq n-1 \right\} .$$

Proof. Consider the splitting $L = \hat{L}_1 \perp \cdots \perp \hat{L}_{t'}$.

First suppose that $r(L_{k,k+1}) \neq 1, 3$ for any k. Then, for each i, $\hat{L}_i$ satisfies either $\dim \hat{L}_i = 1$ or $\hat{L}_i \cong \langle 2^r\varepsilon \rangle \langle 1, 2^{r'_2}\beta_2, \cdots, 2^{r'_m}\beta_m \rangle$ with each r'_j even, and the result follows from 2.4 and 2.5. On the other hand, if $r_s - r_t \neq 2, 4$ for any s and t, then for each i, $\hat{L}_i$ satisfies one of following: $\dim \hat{L}_i = 1$, $\dim \hat{L}_i = 2$, or $\hat{L}_i \cong \langle 2^r\varepsilon \rangle \langle 1, 2^{r'_2}\beta_2, \cdots, 2^{r'_m}\beta_m \rangle$ with each of the r'_j a multiple of 3. The result then follows from 2.4 and 2.6.

REMARK 2.8. The result of 2.7 may not be true for a lattice L satisfying the hypotheses of 2.2. For example, consider $L = \langle 1, 2, 4 \rangle$ over the field $F = \boldsymbol{Q}_2$. In this case, the binary sublattices $L_{j,j+1}$ do not carry all the information about $\theta(0^+(L))$. Indeed, $\theta(0^+(L)) = \dot{F}$, while the right hand side in Theorem 2.7 only gives those field elements $c \neq 0$ such that the Hilbert symbol $(c, -2) = +1$.

III. Higher dimensional cases—Arbitrary components. In this section we handle the remaining cases in which L is a lattice of dimension $\geqq 3$ with at least one Jordan component of dimension $\geqq 2$. For most cases, it suffices to examine the orders of the elements $Q(v)$, $v \in L_i$ for each component L_i.

Following [4], let $A(\alpha, \beta)$ denote the lattice with matrix $\begin{pmatrix} \alpha & 1 \\ 1 & \beta \end{pmatrix}$, for $\alpha, \beta \in F$. Then all of the unimodular binary lattices over F are isometric to one of the following:

$$A(0, 0),\ A(1, 0),\ A(2, 2\rho),\ A(1, 4\rho),\ A(\varepsilon, 2\delta) \text{ where } \varepsilon, \delta \in \mathfrak{U}\,.$$

DEFINITION 3.1. A lattice L has "even order" if $Q(P(L)) \subseteqq \mathfrak{U}\dot{F}^2$; L has "odd order" if $Q(P(L)) \subseteqq 2\mathfrak{U}\dot{F}^2$.

PROPOSITION 3.2. *Let L be unimodular.*
(1) *Suppose* $\dim L = 2$. *Then*

$$L \text{ has odd order} \Longleftrightarrow L \cong A(0, 0) \text{ or } L \cong A(2, 2\rho)\,,$$
$$L \text{ has even order} \Longleftrightarrow L \cong A(1, 0) \text{ or } L \cong A(1, 4\rho)\,.$$

(2) *Suppose* $\dim L \geqq 3$. *Then*

$$\theta(0^+(L)) \neq \dot{F} \Longrightarrow L \text{ has odd order}\,.$$

Proof. Note that $\theta(0^+(L)) = \mathfrak{U}\dot{F}^2$ forces the parity of all elements of $Q(P(L))$ to be the same.

Suppose that $L \cong A(0, 0)$, $A(1, 4\rho)$, $A(2, 2\rho)$, $A(1, 0)$. Then $\theta(0^+(L)) = \mathfrak{U}\dot{F}^2$ (see [2]) and the lattice L has odd or even order depending upon whether L is improper or proper, respectively. But if $L \cong A(\varepsilon, 2\delta)$ then $\theta(0^+(L)) = Q[1, d]\dot{F}^2$ where $d = \det L$, by Proposition B of [2]. Since $d \neq -1, -\Delta$, there is $\beta \in \mathfrak{U}$ for which $(2\beta, -d) = +1$; that is, $2\beta \in Q[1, d]\dot{F}^2$. Thus, $\theta(0^+(L)) \not\subseteq \mathfrak{U}\dot{F}^2$. This completes proof of 1).

Now let $\dim L \geqq 3$. By Proposition A in [2], if $\theta(0^+(L)) \neq \dot{F}$ then L is improper. So, L is split by $A(0, 0)$ (see 93: 18, [4]), and $A(0, 0)$ primitively represents all prime elements. Hence, L must have odd order.

LEMMA 3.3. *Suppose that L has odd order, and the norm $\mathfrak{n}L$ of L is contained in $2\mathfrak{o}$, then the lattices $K = A(0, 0) \perp L$ and $M = A(2, 2\rho) \perp L$ both have odd order.*

Proof. First, consider K. Let $v \in P(K)$ where $v = Ax + By + z$, with $A, B \in \mathfrak{o}$ and $z \in L$. (a) Suppose $\operatorname{ord} Q(z) < \operatorname{ord}(2AB)$. $S_v \in 0(K)$ gives $2B(v, K) \subseteqq Q(v)\mathfrak{o}$. If $Ax + By$ is maximal, say $A \in \mathfrak{U}$, then, $B(v, y)$ is a unit and $Q(z)$ and $Q(v)$ are both prime elements. If $Ax + By$ is nonmaximal, then z is maximal. But, $z \in P(L)$ since $2B(z, L) \subseteqq 2B(v, K) \subseteqq Q(v)\mathfrak{o} = Q(z)\mathfrak{o}$. As L has odd order, this completes this case. (b) Suppose $\operatorname{ord} Q(z) \geqq \operatorname{ord}(2AB)$. This time $S_v \in 0(K)$ yields $2B(v, K) \subseteqq Q(v)\mathfrak{o} \subseteqq (2AB)\mathfrak{o}$. In particular, $2B(v, y) = 2A$. Hence, B is a unit. Similarly, A is a unit. Hence, $\operatorname{ord} Q(v) = 1$.

Next, consider M, and let v be as above. The case for $\operatorname{ord} Q(z) < \operatorname{ord} Q(Ax + By)$ is easier so we suppose $\operatorname{ord} Q(z) \geqq \operatorname{ord} Q(Ax + By)$.

This time $S_v \in 0(M)$ gives $2B(v, M) \subseteq Q(v)\mathfrak{o} \subseteq Q(Ax + By)\mathfrak{o}$. A straightforward calculation shows the case of neither A nor B is a unit can not occur. But, if either A or B is a unit, then $\operatorname{ord} Q(Ax + By) = 1$. When A (resp. B) is a unit, then $2B(v, y) = 2(A + 2\rho B)$ (resp. $2B(v, x) = 2(2 + B)$) shows $\operatorname{ord} Q(v) = 1$.

LEMMA 3.4. *Suppose that L has even order, $\mathfrak{s}L \subseteq 2\mathfrak{o}$. Then $A(1, 0) \perp L = K$ and $A(1, 4\rho) \perp L$ both have even order.*

Proof. We treat only the case K. As before, consider a vector $v \in P(K)$ with $v = Ax + By + z$, $A, B \in \mathfrak{o}$, $z \in L$.

(1) Suppose $\operatorname{ord} Q(z) < \operatorname{ord}(A^2 + 2AB)$. If $Ax + By$ were a maximal vector in $A(1, 0)$, then $2B(v, K) = 2\mathfrak{o}$ and we deduce $Q(z) \in 2\mathfrak{U}$. But, L has even order and so a contradiction. Thus, $Ax + By$ is not maximal which means z is. $S_v \in 0(K)$ implies then $z \in P(L)$. Thus, $\operatorname{ord} Q(v) = \operatorname{ord} Q(z)$ is even.

(2) Suppose $\operatorname{ord} Q(z) \geqq \operatorname{ord}(A^2 + 2AB)$. This time we have $2B(v, x)\mathfrak{o} = 2(A + B)\mathfrak{o} \subseteq (A^2 + 2AB)\mathfrak{o}$. If A is a unit, then so is $Q(v)$. If B is a unit, then the containment forces A also to be a unit, and again $Q(v)$ becomes a unit. Thus, the only possibility is that $\operatorname{ord} A = 1$ and $\operatorname{ord} B \geqq 1$. But, in this case $\operatorname{ord} Q(v) = \operatorname{ord}(A^2 + 2AB) = 2$.

LEMMA 3.5. *Suppose that L has even order, $\mathfrak{s}L \subseteq 2\mathfrak{o}$. Then, for $\varepsilon \in \mathfrak{U}$, we have $K = \langle \varepsilon \rangle \perp L$ has even order.*

Proof. Consider the vector $v \in P(K)$ where $v = Ax + y$, $A \in \mathfrak{o}$, $y \in L$. The case of $A \in \mathfrak{U}$ is trivial. So, let $A \notin \mathfrak{U}$. Then, $y \in P(L)$ so if $\operatorname{ord} Q(v) = \operatorname{ord} Q(y)$ the result follows since L has even order. But, if $\operatorname{ord} Q(y) = \operatorname{ord} A^2$, then $S_v \in O(K)$ gives $\operatorname{ord} 2B(v, x) = \operatorname{ord} 2A \geqq \operatorname{ord} Q(v) \geqq \operatorname{ord} A^2$, forcing $\operatorname{ord} A = 1$ and $\operatorname{ord} Q(v) = 2$.

LEMMA 3.6. *Suppose that L has odd order, and $\mathfrak{s}L \subseteq 4\mathfrak{o}$. Then, for $\varepsilon \in \mathfrak{U}$, the lattice $K = \langle 2\varepsilon \rangle \perp L$ has odd order.*

Proof. Follows as in 3.5. Or, scale by a factor 1/2 and apply 3.5.

LEMMA 3.7. *Let L be unimodular with odd order* $\dim L \geqq 3$; *let L' have odd order, $\mathfrak{n}L' \subseteq 2\mathfrak{o}$. Then, $K = L \perp L'$ has odd order.*

Proof. L is isometric to either $A(0, 0) \perp \cdots \perp A(0, 0)$ or to $A(0, 0) \perp \cdots \perp A(2, 2\rho)$. In any case, Lemma 3.3 applies.

Now, let L be an arbitrary lattice with Jordan splitting $L = L_1 \perp \cdots \perp L_t$ with $\dim L_k \geqq 2$ for at least one k. We determine $\theta(0^+(L))$:

THEOREM 3.8. *Suppose at least one L_i has dimension $\geqq 3$. Then, $\theta(0^+(L)) = \dot{F}$ unless L_j has odd order for all $j = 1, \cdots, t$. In the exceptional case, $\theta(0^+(L)) = \mathfrak{U}\dot{F}^2$.*

Proof. If L has a component L_i of dim $\geqq 3$ of even order, then [2] gives $\theta(0^+(L_i)) = \dot{F}$. So, we may assume that any component L_i of dim $\geqq 3$ has odd order, in which case [2] gives $\theta(0^+(L_i)) = \mathfrak{U}\dot{F}^2$. Then if L has only components L_j of even order, $\theta(0^+(L)) = \dot{F}$. The only other possibility is that L has a binary component of the kind $2^rA(\varepsilon, 2\delta)$ with $\varepsilon, \delta \in \mathfrak{U}$, and $r \geqq 0$. But any such component primitively represents elements of both odd and even order. So, it remains to show that if all Jordan components of L have odd order, then L has odd order, thereby $\theta(0^+(L)) = \mathfrak{U}\dot{F}^2$. This result follows from 3.3, 3.6 and 3.7 by induction on the number t of Jordan components.

We need some more lemmas in order to handle the case of a Jordan splitting with $\dim L_i \leqq 2$ for every i.

LEMMA 3.9. *Suppose $L = M \perp 2^rM'$ where $M \cong A(a, 2b)$, $M' \cong A(a', 2b')$ and a, b, a', b' are units, and $0 < r \leqq 3$. Then, $\theta(0^+(L)) = \dot{F}$.*

Proof. Let M and M' above be adapted to bases $\{x, y\}$, $\{u, v\}$ respectively. First note that $\theta(0^+(M)) = \{c \in \dot{F} \mid (c, 1 - 2ab)) = +1\}$. L contains the sublattices $L_1 = \mathfrak{o}x \perp \mathfrak{o}u \cong \langle a, 2^ra'\rangle$ and $L_2 = \mathfrak{o}x \perp \mathfrak{o}v \cong \langle a, 2^{r+1}b'\rangle$. If $r = 1$ or 3, consider L_1. Every rotation of L_1 extends trivially to a rotation of L so that $\theta(0^+(L)) \supseteqq \theta(0^+(L_1))$. The latter is just the set $\{f \in \dot{F} \mid (f, -2aa') = +1\}$. But, $\Delta \notin \theta(0^+(L_1))$. Hence, $\theta(0^+(L)) = \dot{F}$.

If $r = 2$, consider L_2. We claim that every vector $w = Ax + Bv$ in $P(L_2)$ also yields $w \in P(L)$. If this claim is verified, then once again $\theta(0^+(L))$ contains $\theta(0^+(L_2))$ and the same argument as before prevails. To show this claim, let $z = c_1x + c_2y + c_3u + c_4v$, each $c_i \in \mathfrak{o}$. Since $w \in P(L_2)$ it suffices to check that $2B(w, c_2y + c_2u) \in Q(w)\mathfrak{o}$. This one checks routinely.

LEMMA 3.10. *Suppose $L = M \perp 2^4M'$, where M, M' as in Lemma 3.9. If the spaces FM and FM' are nonisometric, then $\theta(0^+(L)) = \dot{F}$.*

Proof. Put $d = -\det M$. Scaling permits us to assume $a = 1$. As $\theta(0^+(M))$ already has index two in $\dot{F}$, it suffices to show $\theta(0^+(L))$ catches an element in $\dot{F}$ not represented by the binary space $FM \cong [1, -d]$. Since FM and FM' are nonisometric, $Q(M')$ is not contained in $Q(M)$. Since every maximal vector of M' lies in fact in $P(M')$, there must be a maximal vector w in M' with $Q(w) \notin Q(FM)$. Clearly, the symmetries S_w and $S_x \in 0(L)$. Now, $\theta(S_w S_x) = Q(w)\dot{F}^2$ is not contained in $\theta(0^+(M)) = Q[1, d]\dot{F}^2$. We are done.

REMARK 3.11. In general, for $L = 2^s M \perp 2^t M'$, where M, M' are as in Lemma 3.9, if the associated spaces $F(2^s M)$ and $F(2^t M')$ are nonisometric, then $\theta(0^+(L)) = \dot{F}$.

LEMMA 3.12. *Suppose* $L = L_1 \perp 2^{r_2} L_2 \perp \cdots \perp 2^{r_t} L_t$ *with*

$$L_i \cong A(a_i, 2b_i)\ , \quad a_i, b_i \in \mathfrak{U}, \text{ and } r_{j+1} - r_j \geqq 5$$

for $j = 1, \cdots, t-1$. *Furthermore, assume the associated subspaces* $F(2^{r_i} L_i)$ *are pairwise isometric. Then,* $\theta(0^+(L)) = \theta(0^+(L_i)) \neq \dot{F}$.

Proof. Let $v \in P(L)$ with $v = \sum_{i=1}^t z_i$, where $z_i = A_i x_i + B_i y_i$, $A_i, B_i \in \mathfrak{o}$, $Q(x_i) = 2^{r_i} a_i$, $2^{r_i}(2b_i) = Q(y_i)$. Let k be a subscript for which $\operatorname{ord} Q(z_k)$ is minimal. Using $S_v \in 0(L)$, in particular, $2B(v, x_k)$ and $2B(v, y_k)$ both lie within $Q(z_k)\mathfrak{o}$. Hence, if $\operatorname{ord} A_k > \operatorname{ord} B_k$, then B_k must be a unit and $Q(z_k) \in 2^{r_k+1}\mathfrak{U}$. And if $\operatorname{ord} A_k \leqq \operatorname{ord} B_k$, then $\operatorname{ord} A_k \leqq 1$, so that $\operatorname{ord} Q(z_k) \leqq 2^{r_k+2}$.

Consider $j > k$. We have $\operatorname{ord} Q(z_j) \geqq \operatorname{ord} Q(z_k) + 3$. On the other hand, for $j < k$, again using $S_v \in 0(L)$, one sees that both $2^{r_j+1}(A_j + 2B_j b_j)\mathfrak{a}$ and $2^{r_j+1}(A_j a_j + B_j)\mathfrak{o}$ are contained in $2^{r_k}(A_k^2 a_k + 2B_k^2 b_k + 2A_k B_k)\mathfrak{a}$. Therefore, A_j, B_j are both inside $2^{r_k - r_j - 1}(A_k^2 a_k + 2B_k^2 b_k + 2A_k B_k)\mathfrak{o}$. When A_k is a unit, i.e. $\operatorname{ord} Q(z_k) = 2^{r_k}$, then A_j^2, B_j^2, and $A_j B_j$ belongs to $2^{2(r_k - r_j - 1)}\mathfrak{o}$ which gives $Q(z_j) \in 2^{r_k - r_j - 2} 2^{r_k}\mathfrak{o} \subseteqq 2^3 Q(z_k)\mathfrak{o}$. And when A_k is a nonunit, A_j, B_j are both inside $2^{r_k - r_j}\mathfrak{o}$ which implies $Q(z_j) \in 2^5 2^{r_k}\mathfrak{o} \subseteqq 2^3 Q(z_k)\mathfrak{o}$. Thus, we always have: $\operatorname{ord} Q(v) = \operatorname{ord} Q(z_k)$ and moreover, by Local Square Theorem, $Q(v) \in Q(z_k)\dot{F}^2$. Hence, $\theta(0^+(L)) = Q(F(2^{r_k} L_k)\dot{F}^2 = \theta(0^+(L_i))$ for any i.

REMARK 3.13. Since for any i, $\theta(0^+(L_i)) = Q[1, -d_i]\dot{F}^2$, where $d_i = -\det L_i = 1 - 2a_i b_i$. In particular, $\Delta\dot{F}^2 \in \theta(0^+(L_i))$. The same proof, therefore, extends the validity of Lemma 3.12 to the case where we require that the exponents satisfy: $r_{j+1} - L_j \geqq 4$ for $j = 1, \cdots, t-1$. All other conditions remain unchanged.

Summarizing, we have the following theorem:

THEOREM 3.14. *Suppose* $L = L_1 \perp 2^{r_2} L_2 \perp \cdots \perp 2^{r_t} L^t$ *is a Jordan* *splitting for* L, *and* $\dim L_i \leqq 2$ *for every* i *and with at least one component, say* L_{i_0} *being binary. Then,* $\theta(0^+(L))$ *is determined as follows*:

(i) *If all* L_i *have odd* (or all have even) *order, then* $\theta(0^+(L)) = \mathfrak{U}\dot{F}^2$.

(ii) *If there is a binary component* L_j *with odd* (even) *order and a component* L_k *with even* (odd) *order, then* $\theta(0^+(L)) = \dot{F}$.

(iii) *Suppose* $L_i \cong A(a_i, 2b_i)$ *for some* i *with* $a_i, b_i \in \mathfrak{U}$,

(a) *If there is a binary component of either odd or even order, then* $\theta(0^+(L)) = \dot{F}$.

(b) *If there is some* $L_j \cong A(a_j, 2b_j)$ *such that the associated spaces* $F(2^{r_i}L_i)$ *and* $F(2^{r_j}L_j)$ *are nonisometric, then* $\theta(0^+(L)) = \dot{F}$.

(iv) *Suppose* $L_i \cong A(a_i, 2b_i)$ *whenever* $\dim L_i = 2$, *then* $\theta(0^+(L)) \neq \dot{F}$ *if and only if*

(a) *the associated spaces of all binary components are isometric,*

(b) *for any unary component, say* $L_k = \langle \varepsilon_k \rangle$, $\varepsilon_k \in \mathfrak{U}$, *the Hilbert symbol* $(2^{r_k}\varepsilon_k, -\det L_{i_0}) = +1$, *and*

(c) $r_{j+1} - r_j \geqq 4$ *for* $j = 1, \cdots, t-1$.

In the exceptional case described in iv) *we actually have* $\theta(0^+(L)) = \theta(0^+(L_{i_0})) = \{c \in \dot{F} \mid (c, -\det L_{i_0}) = +1\}$.

REMARK 3.15. After a Jordan decomposition for $L = J_1 \perp \cdots \perp J_t$ is obtained, the forms of the components can be easily determined. In case the dimension of J_i is greater or equal to 3 it suffices to check whether J_i is proper or improper. In the binary cases, it suffices to compute $\mathfrak{n}J_i$, $\mathfrak{s}J_i$ and the associated spaces FJ_i

IV. Application to a theorem of Kneser. In this section we apply the results of §§ II and III to improve a theorem of Kneser [3, Satz 5], which gives sufficient conditions, in terms of the reduced determinant (à la Eichler [1]), for an indefinite lattice over $\boldsymbol{Z}$ to have class number 1.

The notation of this section will conform to that of [4]. In particular, when L is a lattice over $\boldsymbol{Z}$, $\mathfrak{n}L$ denotes the $\boldsymbol{Z}$-module generated by the subset $Q(L)$ of $\boldsymbol{Q}$. Define the *reduced determinant* $d'L$ to be the determinant of the lattice obtained from L by scaling by a^{-1} where $\mathfrak{n}L$ is generated by a. The formulation of the original Kneser's theorem will be modified to conform to our notational conventions and is stated here for reference.

THEOREM (Kneser). *Let* L *be an indefinite lattice over* $\boldsymbol{Z}$ *with* $\dim L = n \geqq 3$. *If* $d'L = \pm \prod_p p^{s_p}$ *and* (i) $s_p < n(n-1)/2$ *whenever* p *is odd, and* (ii) $s_2 < n(n-3)/2 + [(n+1)/2] = b_2$ (where [ ] denotes the greatest integer function), *then the class number* $h(L) = 1$.

The bounds given for s_p for p odd are the best possible. However, we now show that the bound b_2 can be considerably improved. Furthermore, the new bounds obtained here will be shown to be the *best possible*.

THEOREM 4.2. *Suppose L is indefinite over $\boldsymbol{Z}$, and* $\dim L = n \geqq 3$. *If* $d'L = \pm \prod_p p^{s_p}$ *and* (i) $s_p < n(n-1)/2$ *whenever p is odd, and* (ii) $s_2 < n(n-1) = b'_2$, *then* $h(L) = 1$.

We break the proof of the theorem into two parts which we state separately as lemmas.

LEMMA 4.3. *Let L be as in the theorem. If L satisfies condition* (i) *and if the localization L_2 of L at $p = 2$ has a Jordan component L'_2 which has* $\dim L'_2 \geqq 2$, *then* $h(L) = 1$.

Proof. The condition (i) assures that $\theta(0^+(L_p)) \supseteqq \mathfrak{U}_p\dot{\boldsymbol{Q}}_p^2$ whenever p is odd. If $\dim L'_2 \geqq 3$ or if $\dim L'_2 = 2$ with $L'_2 \not\cong 2^t A(a, 2b)$, $a, b \in \mathfrak{U}_2$, then $\theta(0^+(L_2)) \supseteqq \mathfrak{U}_2\dot{\boldsymbol{Q}}_2^2$ (see [2]) and $h(L) = 1$.

So we assume $L'_2 \cong 2^t A(a, 2b)$ with $a, b \in \mathfrak{U}_2$. Then the index $[\dot{\boldsymbol{Q}}_2/\dot{\boldsymbol{Q}}_2^2 \colon \theta(0^+(L'_2))] = 2$, so that either $\theta(0^+(L_2)) = \dot{\boldsymbol{Q}}_2$ or

$$\theta(0^+(L_2)) = \theta(0^+(L'_2)) = \{c \in \boldsymbol{Q}_2 \mid (c, -\det L'_2)_2 = +1\} .$$

In the first case, the proof is finished; for the second case, note that $\theta(0^+(L_2)) \cap \mathfrak{U}_2\dot{\boldsymbol{Q}}_2^2 = \dot{\boldsymbol{Q}}_2^2 \cup 5\dot{\boldsymbol{Q}}_2^2$ since $-\det L'_2 \in \mathfrak{U}_2\dot{\boldsymbol{Q}}_2^2 \backslash 5\dot{\boldsymbol{Q}}_2^2$.

Now, in the indefinite situation $h(L)$ is equal to the order of the factor group $J_Q/P_Q J_Q^L$. So in the remaining case above, take an element $i \in P_Q J_Q^L$. Since $J_Q = P_Q J_Q^S$, it suffices to take i to belong to J_Q^S, i.e. $i_p \in \mathfrak{U}_p$ for all finite primes p. If $i_2 \in \dot{\boldsymbol{Q}}_2^2 \cup 5\dot{\boldsymbol{Q}}_2^2$, then $i \in J_Q^L$; if $i_2 \in 3\dot{\boldsymbol{Q}}_2^2 \cup 7\dot{\boldsymbol{Q}}_2^2$, then $i \in (-1)J_Q^L$.

LEMMA 4.4. *Let L be as in the theorem. If L satisfies condition* (i) *and if* $h(L) \neq 1$, *then* $s_2 \geqq n(n-1)$.

Proof. By 4.3, L_2 must have a Jordan splitting consisting of only 1-dimensional components, say

$$2^{-k}L_2 \cong \langle \varepsilon_1 \rangle \perp \langle 2^{r_2}\varepsilon_2 \rangle \perp \cdots \perp \langle 2^{r_n}\varepsilon_n \rangle$$

with $\varepsilon_i \in \mathfrak{U}_2$, $r_i \in \boldsymbol{Z}$ with $0 = r_1 < r_2 < \cdots < r_n$ and $k = \operatorname{ord}_2(a)$ where $\mathfrak{n}L_2 = a\boldsymbol{Z}_2$.

It suffices to verify that $r_j \geqq 2(j-1)$ for $j = 3, \cdots, n$, and that $r_2 + r_3 \geqq 6$. If $r_2 = 1$ and $r_3 \leqq 5$ or if $r_2 = 2$ and $r_3 = 3$, it follows from 2.2 that $\theta(0^+(L_2)) \supseteqq \mathfrak{U}_2\dot{Q}_2^2$. So, in any case, $r_3 \geqq 4$ as desired and $r_2 + r_3 \geqq 6$.

Assume that $r_j \geqq 2(j-1)$ for $j = 3, \cdots, m < n$, and verify that $r_{m+1} \geqq 2m$. First note that if $r_m \geqq 2m$, then the result is immediate. So, $r_m = 2m - 2$ or $r_m = 2m - 1$, and $r_m - r_{m-1} \leqq 3$. If $r_m - r_{m-1} = 1$ or 2, then arguing as above gives $r_{m+1} \geqq r_{m-1} + 4$ as desired. If $r_m - r_{m-1} = 3$, then $r_m = 2m - 1$ and $r_{m+1} \geqq 2m$.

Thus $r_j \geqq 2(j-1)$ for $j = 3, \cdots, n$. The result follows as

$$s_2 = \sum_{j=1}^{n} r_j \geqq 6 + \sum_{j=4}^{n} r_j \geqq 6 + 2\sum_{j=4}^{n} (j-1) = 2\sum_{j=1}^{n} (j-1) = n(n-1) .$$

REMARK 4.5. Although the difference $b_2' - 2b_2$ tends to infinity as n grows large, one sees $\lim_{n\to\infty} b_2'/2b_2 = +1$. The bound b_2' is the best possible for any value of n because the lattice $L \cong \langle -7, 2^2, 2^4, \cdots, 2^{2(n-1)}\rangle$ satisfies the condition (i) of 4.2 but has class number 2 and $s_2 = n(n-1)$. [Strictly speaking, we should be discussing in terms of *proper* class number; of course, when n is odd there is no distinction.] When L is a definite lattice, there is an analogous theorem giving sufficient conditions for $g^+(L) = 1$ (the number of proper spinor genera in the genus of L). The bound b_2'' obtained there is not as large as b_2' because such a lattice may have binary 2-adic Jordan components but still not have $g^+(L) = 1$. See a comparison table given below.

THEOREM 4.6. *Suppose L is a definite lattice over $\boldsymbol{Z}$ with* $\dim L = n \geqq 3$. *If $d'L = \pm \prod_p p^{s_p}$ and* (i) *$s_p < n(n-1)/2$ whenever p is odd, and* (ii) *$s_2 < n(n-3) + 2[(n+1)/2] = b_2''(=2b_2)$, then $g^+(L) = 1$.*

The proof follows from 3.14 using an argument analogous to the proof of [3, Satz 5].

REMARK 4.7. The bound b_2'' is again the best possible for any value of n since the lattice $L \cong \langle 1, 1, 2^4, 2^4, 2^8, \cdots, 2^{2k}\rangle$ with $k = [(n-1)/2]$, satisfies the condition (i) of 4.6 but has $g^+(L) = 2$ and $s_2 = n(n-3) + 2[(n+1)/2]$.

TABLE 4.8.

n	b_2	b_2''	b_2''
3	2	4	6
4	4	8	12
5	8	16	20
6	12	24	30
7	18	36	42
8	24	48	56
9	32	64	72
10	40	80	90

References

1. M. Eichler, *Quadratische Formen und orthogonale Gruppen*, Berlin-gottingen-Heidelberg: Springer, 1952.
2. J. S. Hsia, *Spinor norms of local integral rotations, I*, Pacific J. Math., **57** (1975), 199-206.
3. M. Kneser, *Klassenzahlen indefiniter quadratischer Formen in drei order mehr Veranderlichen*, Arch. Math., (1956), 323-332.
4. O. T. O'Meara, *Introduction to Quadratic Forms*, Berlin-Gottingen-Heidelberg: Springer, 1963.
5. O. T. O'Meara and B. Pollak, *Gneration of local integral orthogonal groups*, Math. Zeitschr., **87** (1965), 385-400.

Received April 30, 1975.

Ohio State University

Printed in Japan by International Academic Printing Co., Ltd., Tokyo, Japan

Pacific Journal of Mathematics

Vol. 61, No. 1 November, 1975