ON THE INTEGRAL EXTENSIONS OF QUADRATIC FORMS OVER LOCAL FIELDS

MELVIN BAND

I. Introduction. Let F be a local field with ring of integers $\mathcal{O}$ and unique prime ideal (p). Suppose that V is a finite-dimensional regular quadratic space over F, W and W' are two isometric subspaces of V (i.e. $\tau: W \to W'$ is an isometry from W to W'). By the well-known Witt's Theorem, τ can always be extended to an isometry $\sigma \in O(V)$.

The integral analogue of this theorem has been solved over non-dyadic local fields by James and Rosenzweig [**2**], over the 2-adic fields by Trojan [**4**], and partially over the dyadics by Hsia [**1**], *all* for the special case that W is a line. In this paper we give necessary and sufficient conditions that two arbitrary dimensional subspaces W and W' are integrally equivalent over non-dyadic local fields. We let τ be the isometry between W and W' and we search for an integral isometry $\sigma \in O(V)$ such that $\sigma|W = \tau$.

II. Notation and basic concepts. The language and notation used in this paper is geometric and follows quite closely with the notation used in [**3**], thus we can reformulate the problem using O'Meara's notation as follows: Let V be a regular quadratic space over a non-dyadic local field F, and let L be a lattice on V. Let W and W' be isometric sublattices on L. Then we search for necessary and sufficient conditions that an isometry σ belonging to $O(L)$ exists such that $\sigma|W = \tau$.

For any sublattice J in L, we define $s(J)$ to be the ideal generated by $J \cdot J$, $J^{(p^k)} = \{x \in J | \, x \cdot J \subseteq (p^k)\}$ and $J^{\perp} = \{x \in L | \, x \cdot J = \{0\}\}$. The lattice L admits a Jordan decomposition into modular sublattices $L = L_1 \oplus L_2 \oplus L_3 \oplus \ldots \oplus L_t$ such that $s(L_1) \supset s(L_2) \supset \ldots \supset s(L_t)$. If $L = \sum \oplus L_i$ is an arbitrary Jordan decomposition such that $s(L_i) = (p^i)$ and if L_i is non-empty, then we define the rth Jordan chain associated with the given splitting of L to be $L_{(r)} = \sum_{i \leqq r} L_i$ and the rth inverse chain of L to be $L_{(r)}^{\perp} = \sum_{i > r} L_i$. Then $L = L_{(r)} \perp L_{(r)}^{\perp}$. James and Rosenzweig, in [**2**], decomposed vectors into critical components as described in the following manner. Let v be a primitive vector of L. Then there exists a Jordan decomposition of $L = \sum L_i'$ such that $s(L_i') = (p^i)$ if L_i' is non-empty in which

$$v = \sum_{i=1}^{k} p^{f_i} v_{\lambda_i} \qquad (v_{\lambda_i} \text{ is a primitive basis vector in } L_{\lambda_i}', v_{\lambda_i} \neq 0)$$

satisfies the following properties:

Received December 31, 1968.

https://doi.org/10.4153/CJM-1970-037-x Published online by Cambridge University Press

(A) $f_1 > f_2 > f_3 > \ldots > f_k = 0$;

(B) $f_1 + \lambda_1 < f_2 + \lambda_2 < \ldots < f_k + \lambda_k = \lambda_k$.

The $\{\lambda_i\}$ are called the critical indices and the $\{f_i\}$ are called the critical exponents of v at the critical indices $\{\lambda_i\}$, respectively.

If we define $\operatorname{ord}(v) = \operatorname{ord}(v \cdot L)$ and $\operatorname{ord}_K(v) = \operatorname{ord}(v \cdot L^{(p^K)})$, then James and Rosenzweig [**2**] showed that K is critical for the vector v if

$$\operatorname{ord}_{K-1}(v) = \operatorname{ord}_K(v) = \operatorname{ord}_{K+1}(v) - 1.$$

Note that if two vectors are integrally equivalent, they have:

(1) the same critical indices,

(2) the same critical exponents at their respective critical indices.

For the given vector v, define

$$s_i = \lambda_{i+1} + f_{i+1} - f_i \qquad (i = 1, \ldots, k-1).$$

Let $L = \sum \oplus M_i$ be an arbitrary Jordan decomposition of L such that $s(M_i) = (p^i)$ and let $v = \sum p^{h_i} m_i$, $m_i \in M_i$ being primitive or zero. Then the following is true:

(a) if $l = \lambda_j$, then $h_l = f_j$ $(j = 1, \ldots, k)$;

(b) if $l < \lambda_1$, then $h_l \geqq f_1 + \lambda_1 - l$;

(c) if $\lambda_j < l < \lambda_{j+1}$, then

$$h_l \geqq \begin{cases} f_j & \text{when } \lambda_j \leqq l \leqq s_j, \\ f_{j+1} + \lambda_{j+1} - l & \text{when } s_j \leqq l \leqq \lambda_{j+1}; \end{cases}$$

(d) if $l \geqq \lambda_r$, then $h_l \geqq 0$.

Let $v_{(l)} = \sum_{i \leqq l} p^{h_i} m_i$. Then if v is integrally equivalent to w, (which we shall write $v \sim w$), then

(3) $\operatorname{ord}(v_{(s_j)}{}^2 - w_{(s_j)}{}^2) \geqq s_j + 2f_j$ $(j = 1, \ldots, k-1)$.

James and Rosenzweig showed [**2**] that conditions (1), (2), and (3) are both necessary and sufficient for two primitive vectors of the same length to be integrally equivalent.

Note that if two subspaces W and W' are integrally equivalent (which we shall write $W \sim^{\tau} W'$), then $\eta \in W$ is integrally equivalent to $\eta' \in W'$, where $\eta' = \tau(\eta)$ for all $\eta \in W$. Conversely, we shall show that if $\eta \sim \tau(\eta)$ for all $\eta \in W$, then $W \sim W'$. Since W has infinitely many vectors, it would seem that one cannot make the computations to check for integral equivalence, but by reading through the proofs, one can see that there are actually only finitely many computations to perform in order to check for integral equivalence of quadratic subspaces.

III. Characterization of completely independent vectors having only one critical index.

Remark. Let $W = \mathcal{O}\eta_1 + \ldots + \mathcal{O}\eta_r$ and let $W' = \mathcal{O}\eta_1' + \ldots + \mathcal{O}\eta_r'$, where $\eta_i' = \tau(\eta_i)$. Define

$$w_i = \sum_{j=1}^{r} \alpha_{ij}\eta_j \quad \text{and} \quad w_i' = \sum_{j=1}^{r} \alpha_{ij}\eta_j'.$$

Then $W \sim^{\tau} W'$ if and only if

$$W^{(1)} = \mathcal{O}p^{a_1}w_1 + \ldots + \mathcal{O}p^{a_r}w_r \sim^{\tau} W^{(1)'} = \mathcal{O}p^{a_1}w_1' + \ldots + \mathcal{O}p^{a_r}w_r'.$$

Hence, throughout the article we will not distinguish between W and $W^{(1)}$.

Definition. Let $\eta_1, \ldots, \eta_r$ be a set of vectors in $L = \sum L_i$ and suppose that each $\eta_j = \sum p^{a_{ji}}u_{ji}$ ($u_{ji} \in L_i$ being primitive). Let each vector η_j have a first critical index at j_1 with critical exponent a_{jj_1}. Then $\eta_1, \ldots, \eta_r$ are called completely independent if $u_{11_1}, \ldots, u_{rr_1}$ are linear independent over the residue class field $\mathcal{O}/(p)$.

Since, by necessity, every $\eta \in W$ is integrally equivalent to $\tau(\eta) \in W'$, the basis vectors of W are completely independent if and only if the basis vectors of W' are completely independent.

LEMMA 1. *There exists a set of basis vectors $\tau_1, \ldots, \tau_r$ of W which are completely independent.*

Proof. By induction on the dimension of W. If $\dim W = 1$, the proof is trivial. Hence assume that the lemma is true if $\dim W = r - 1$, i.e., $W = \mathcal{O}\eta_1 + \mathcal{O}\tau_2 + \ldots + \mathcal{O}\tau_r$ and $\tau_2, \ldots, \tau_r$ are completely independent. Choose $\tau_1 = c_1\eta_1 - \sum c_i\tau_i$ ($c_1, \ldots, c_r \in \mathcal{O}$), so that $\tau_1, \ldots, \tau_r$ are completely independent.

Before characterizing completely independent vectors each having only one critical index, we state the following useful result.

LEMMA 2. *If L contains the $\mathfrak{A}$-modular sublattice J, then J splits L if and only if $J \cdot L \subseteq \mathfrak{A}$.*

Proof. See [**3**, 82:15].

LEMMA 3. *Let η be a primitive vector in L having only one critical index at s. Suppose further that* $\operatorname{ord}(\eta^2) > s$. *Then there exists a vector $t \in L$ such that $\eta \cdot t = p^s$, $t^2 = 0$.*

Proof. Since η has only one critical index at s, by [**2**] there exists some Jordan decomposition, say $L = \sum L_i'$ such that $\eta \in L_s'$. Choose $\bar{t} \in L_s'$ such that $\eta \cdot \bar{t} = p^s$. Now consider the vector $t = \alpha\eta + \beta\bar{t}$. By an application of Hensel's Lemma, we can choose α and β in $\mathcal{O}$ so that t satisfies the required properties.

LEMMA 4. *Let $\eta_1, \ldots, \eta_r$ be a set of primitive vectors, each having only one critical index at s, and are completely independent. Suppose further that* $\operatorname{ord}(\eta_i \cdot \eta_j) > s$. *Then there exists a set of vectors $\{t_i\}$ such that*

(1) $t_i \cdot \eta_i = p^s$,

(2) $t_i \cdot \eta_j = 0$ ($i \neq j$),

(3) $t_i \cdot t_j = 0$ ($1 \leqq i, j \leqq r$).

https://doi.org/10.4153/CJM-1970-037-x Published online by Cambridge University Press

Proof. By scaling, if necessary, we can assume that $s = 0$. By Lemma 3, we can choose $t_1' \cdot \eta_1 = 1, t_1'^2 = 0$. Then $L = \mathcal{O}\eta_1 + \mathcal{O}t_1' \perp L_c'$. Now each vector η_j $(j \geqq 2)$ can be written in the following way:

$$\eta_j = \alpha_j\eta_1 + \beta_j t_1' + \eta_j', \qquad \eta_j' \in L_c';$$
$$\eta_j \cdot \eta_1 = \alpha_j \eta_1^2 + \beta_j \in (p) \Rightarrow \beta_j \in (p).$$

Therefore, $\eta_2', \ldots, \eta_r'$ are primitive and it is easy to verify that $\eta_2', \ldots, \eta_r'$ satisfy the hypothesis of the lemma in L_c'. Hence, by induction on the dimension of L, there exists a set of vectors $t_2, \ldots, t_r \in L_c'$ which satisfies the lemma for the vectors $\eta_2', \ldots, \eta_r'$. Therefore

$$t_i \cdot \eta_i = 1 \qquad (i = 2, \ldots, r),$$
$$t_i \cdot \eta_j = 0 \qquad (i \neq j)\ (i = 2, \ldots, r),$$
$$t_i \cdot t_j = 0.$$

But $L = \mathcal{O}\eta_1 + \mathcal{O}(t_1' - \sum c_i t_i) \perp L_c''$, provided $c_2, \ldots, c_r \in \mathcal{O}$. Choose $c_2, \ldots, c_r \in \mathcal{O}$ so that $t_1 = t_1' - \sum c_i t_i$ is orthogonal to the vectors $\{\eta_2, \ldots, \eta_r\}$. Thus $t_1, \ldots, t_r$ satisfy the required properties.

LEMMA 5. *Let the basis vectors of W be primitive, have only one critical index at* 0, *and be completely independent. Then there exists a set of basis vectors* $w_1, \ldots, w_r$ *of W which are completely independent, have only one critical index at* 0, *and the following holds true:*

$$L = \mathcal{O}w_1 \perp \mathcal{O}\bar{w}_2 \perp \ldots \perp \mathcal{O}\bar{w}_s \perp \mathcal{O}w_{s+1} + \mathcal{O}t_{s+1} \perp \ldots \perp \mathcal{O}\bar{w}_r + \mathcal{O}t_r \perp L_c,$$

where $t_i \cdot w_i = 1$, $t_i \cdot w_k = 0$ $(i \neq k)$, $t_i^2 = 0$ *and*

$$w_i = \sum_{k=1}^{i} \alpha_{ik}\bar{w}_k \qquad (i \leqq s),$$
$$w_i = \sum_{k=1}^{s} \alpha_{ik}\bar{w}_k + \sum_{k=s+1}^{i-1} \alpha_{ik}t_k + \bar{w}_i \quad (i > s).$$

Proof. Suppose that $W = \mathcal{O}\eta_1 + \ldots + \mathcal{O}\eta_r$, where $\eta_1, \ldots, \eta_r$ are completely independent. We consider three cases.

Case 1. Suppose that one of the vectors, say η_1, satisfies the property that $|\eta_1^2| = 1$. Then let $w_1 = \eta_1$. Thus $L = \mathcal{O}w_1 \perp L_c'$. Then

$$\eta_j = \alpha_j w_1 + \eta_j' \qquad (j = 2, \ldots, r),$$

where $\eta_j' \in L_c'$. Then $\{\eta_j'\}$ satisfies the hypothesis of the lemma in L_c' and so by induction our proof is complete.

Case 2. Suppose that $|\eta_i^2| < 1$ $(1 \leqq i \leqq r)$ but two vectors, say $|\eta_1 \cdot \eta_2| = 1$, then let $w_1 = \eta_1 + \eta_2$. Then $L = \mathcal{O}w_1 \perp L_c''$. Write

$$\eta_i = \alpha_i w_1 + \eta_i'', \qquad \eta_i'' \in L_c'' \quad (i = 2, \ldots, r).$$

Since $\{\eta_i''\}$ are completely independent, a simple induction on the dimension of the lattice completes the proof.

https://doi.org/10.4153/CJM-1970-037-x Published online by Cambridge University Press

Case 3. We are only left with the case that $|\eta_i \cdot \eta_j| < 1$ $(1 \leqq i, j \leqq r)$. But this has been proved by Lemma 4.

COROLLARY. *There exists a decomposition of* $L = \sum L_i'$ *such that* $W \in L_0'$.

Proof. Note that $\mathscr{O}w_1 \perp \mathscr{O}\bar{w}_2 \perp \ldots \perp \mathscr{O}\bar{w}_r + \mathscr{O}t_r$ is a unimodular sublattice of L.

LEMMA 6. *Let* $W = \mathscr{O}\eta_1 + \ldots + \mathscr{O}\eta_r$ *and suppose that each basis vector is primitive and has only one critical index at* 0. *Suppose further that* $\eta_1, \ldots, \eta_r$ *are completely independent. Then there exists a set of vectors* $\{t_i\}$ $(1 \leqq i \leqq r)$ *such that*

(1) $t_i \cdot \eta_i = 1$,
(2) $t_i \cdot \eta_j = 0$ $(i \neq j)$,
(3) $|t_i^2| \leqq 1$ $(1 \leqq i \leqq r)$.

Proof. By renumbering the vectors, if necessary, we can assume that either
(A) $s(W) = s(\mathscr{O}\eta_1)$ or
(B) $s(W) = s(\mathscr{O}(\eta_1 + \eta_2))$ if $s(W) \neq s(\mathscr{O}\eta_j)$ $(j = 1, \ldots, r)$.

Consider case (A). If $\text{ord}(\eta_1^2) > \text{ord}(\eta_1)$, then by Lemma 4 our proof is complete. Thus we can assume that $\text{ord}(\eta_1^2) = \text{ord}(\eta_1)$. Hence $L = \mathscr{O}\eta_1 \perp L_c'$. Write $\eta_j = \alpha_j\eta_1 + \eta_j'$, where $\eta_j' \in L_c'$ $(j = 2, \ldots, r)$. Then it is easy to verify that $\eta_2', \ldots, \eta_r'$ satisfy the hypothesis of the lemma in L_c'. Hence by induction on the dimension of the lattice, there exists a set of vectors $t_2, \ldots, t_r \in L_c'$ satisfying (1), (2), and (3) for the vectors $\eta_2', \ldots, \eta_r'$. Let $t_1' = \eta_1|\eta_1^2|^{-1}$ and define $t_1 = t_1' - \sum_{i=2}^{r} c_i t_i$. By choosing $c_2, \ldots, c_r$ appropriately in $\mathscr{O}$, $t_1, \ldots, t_r$ is the required set.

Case (B). Since $s(W) = s(\mathscr{O}(\eta_1 + \eta_2))$, by Lemma 4 we can assume that $|(\eta_1 + \eta_2)^2| = 1$. Since $w_1 = \eta_1 + \eta_2$, $w_2 = \eta_2, \ldots, w_r = \eta_r$ satisfy the conditions of case (A), there exists a set of vectors $t_1, \ldots, t_r$ which satisfy the lemma for the vectors $w_1, \ldots, w_r$. Then $t_1, t_1 + t_2, t_3, \ldots, t_r$ is the required set.

The following three lemmas are a generalization of Lemmas 4, 5, and 6. Keeping in mind the value of the lower bound of the exponent of a vector at its non-critical indices, these lemmas can be easily proved.

LEMMA 7. *Let* $\eta_1, \ldots, \eta_r$ *be a set of primitive vectors, each having only one critical index at* $k_1, \ldots, k_r$, *respectively, and are completely independent. Suppose that if* $\text{ord}(\eta_i) = \text{ord}(\eta_j)$, *then* $\text{ord}(\eta_i \cdot \eta_j) > \text{ord}(\eta_i)$ $(1 \leqq i, j \leqq r)$. *Then there exists a set of vectors* $\{t_i\}$ *such that* $t_i \cdot \eta_i = p^{k_i}$, $t_i \cdot \eta_j = 0$ $(i \neq j)$ *and* $t_i \cdot t_j = 0$.

LEMMA 8. *Let* $\eta_1, \ldots, \eta_r$ *be a set of primitive vectors, each having only one critical index and are completely independent and such that* $W = \mathscr{O}\eta_1 + \ldots + \mathscr{O}\eta_r$. *Then there exists a set of vectors* $w_1, \ldots, w_r$ *which satisfy the same properties as* $\eta_1, \ldots, \eta_r$ *and such that*

$$L = \mathscr{O}w_1 \perp \mathscr{O}\bar{w}_2 \perp \ldots \perp \mathscr{O}\bar{w}_s \perp \mathscr{O}\bar{w}_{s+1} + \mathscr{O}t_{s+1} \perp \ldots \perp \mathscr{O}\bar{w}_r + \mathscr{O}t_r \perp L_c,$$

where

$$t_i \cdot w_i = p^{k_i},$$
$$t_i \cdot t_j = 0 \qquad (s + 1 \leqq i, j \leqq r),$$
$$t_i \cdot w_j = 0 \qquad (i \neq j),$$

and where

$$w_i = \sum_{j=1}^{i} \alpha_{ij} \bar{w}_j \qquad (i < s),$$

$$w_i = \sum_{j=1}^{s} \alpha_{ij} \bar{w}_j + \sum_{j=s+1}^{i-1} \alpha_{ij} t_j + \bar{w}_i \qquad (i \geqq s), \text{ where } \alpha_{ij} \in \mathcal{O}.$$

Such a set of basis vectors $\{w_i\}$ will be called a *canonical set.*

LEMMA 9. *Let $\eta_1, \ldots, \eta_r$ be a set of primitive vectors, each having only one critical index at $k_1, \ldots, k_r$, respectively. Then there exists a set of vectors $\{t_i\}$ such that*

(1) $t_i \cdot \eta_i = p^{k_i}$,
(2) $t_i \cdot \eta_j = 0$,
(3) $t_i^2 \equiv 0 \pmod{p^{k_i}}$.

The following lemma is the converse of the previous lemma, and thus characterizes completely independent vectors having only one critical index.

LEMMA 10. *Let $\eta_1, \ldots, \eta_r$ be a set of primitive vectors having only one critical index at $k_1, \ldots, k_r$, respectively. Suppose that there exists a set of vectors $\{t_i\}$ such that*

(1) $t_i \cdot \eta_i = p^{k_i}$,
(2) $t_i \cdot \eta_j = 0$,
(3) $t_i^2 \equiv 0 \pmod{p^{k_i}}$.

Then $\eta_1, \ldots, \eta_r$ are completely independent.

PROPOSITION 1. *Let $\eta_1, \ldots, \eta_r$ be a set of vectors of L, such that each η_i has a first critical index, say at k_i, for $1 \leqq i \leqq r$, and suppose that the vectors are completely independent. Then there exists a decomposition $L = \sum L_i'$ such that $\eta_i \in L_{(k_i - 1)}'^{\perp}$ for every i, $1 \leqq i \leqq r$.*

Proof. By renumbering the vectors and scaling, if necessary, we can assume that $\eta_1, \ldots, \eta_{g_1}$ have first critical indices at 0, $\eta_{g_1+1}, \ldots, \eta_{g_2}$ have first critical indices at 1, $\eta_{g_n+1}, \ldots, \eta_r$ have first critical indices at n. By the Corollary to to Lemma 5, there exists a decomposition $L^{[n]}$ of L such that

$$\eta_{g_n+1}, \ldots, \eta_r \in L_{(n-1)}{}^{[n]\perp}.$$

Now consider the vectors $\tau_{g_{n-1}+1} = \eta_{g_{n-1}+1} | L_{(n-1)}{}^{[n]}, \ldots, \tau_{g_n} = \eta_{g_n} | L_{(n-1)}{}^{[n]}$. These vectors have only one critical index at $n - 1$ and are completely independent. Applying again the Corollary to Lemma 5, there exists a decomposition $\sum_{i \leqq n-1} L_i{}^{[n-1]}$ of $\sum_{i \leqq n-1} L_i{}^{[n]}$ such that $\tau_{g_{n-1}+1}, \ldots, \tau_{g_n} \in L_{n-1}{}^{[n-1]}$.

Continuing in this manner we obtain the lattice

$$L = \sum_{i \leqq 0} L_i^{[0]} \perp L_1^{[1]} \perp L_i^{[i]} \perp \ldots \perp L_n^{[n]} \perp \sum_{i>n} L_i^{[n]},$$

which has the required properties.

IV. Selection of basis vectors.

Notation. Throughout the remainder of the article, vectors unprimed will refer to elements associated with W and vectors which are primed, e.g. η', will refer to elements associated with W'. We introduce the following definitions. Define $k_1(\eta)$ and $k_2(\eta)$ to be the first and second critical indices of η, respectively, if they exist. Let $a_1(\eta)$ and $a_2(\eta)$ be the first and second critical exponents of η, respectively, if they exist.

Let $s(\eta)$ denote the number of critical indices of η. Let

$$q(\eta) = \begin{cases} \infty & \text{if } s(\eta) = 1, \\ k_2(\eta) + a_2(\eta) - a_1(\eta) & \text{if } s(\eta) > 1. \end{cases}$$

Choose basis vectors for W as follows: Pick η_1 so that $q(\eta_1)$ is maximum over all basis vectors $\eta \in W$. Assuming that $\eta_1, \ldots, \eta_{g-1}$ have been chosen, let W_g be the set of basis vectors in W which are completely independent from $\eta_1, \ldots, \eta_{g-1}$. Choose η_g in W_g so that $q(\eta_g)$ is maximum over all vectors $\eta \in W_g$. Hence by induction we obtain a completely independent set of vectors. Such a set of basis vectors of W will be called a maximalized set of vectors.

Renumber the basis vectors so that $q(\eta_i) < q(\eta_j)$ implies $i < j$. Decompose each basis vector as follows. Let $\eta_i = p^{a_1(\eta_i)}\tau_i + \bar{\eta}_i$, where $p^{a_1(\eta_i)}\tau_i \in L_{(q(\eta_i))}$ and $\bar{\eta}_i \in L_{(q(\eta_i))}{}^{\perp}$. By multiplying each vector η_i by p^{x_i} for some $x_i \in Z$, we can assume that $a_1(\eta_i) = a_1(\eta_j)$. Now by adding η_j or $-\eta_j$ to η_i $(j > i)$, if necessary, we can assume that the vectors $\{\tau_i\}$ are canonical, and $\eta_1, \ldots, \eta_r$ are a maximalized set, since $q(\eta_i \pm \eta_j) = q(\eta_i)$.

Throughout the remainder of the article, we assume that the basis vectors of W (and, of course, of W' by necessity) are chosen in the above manner.

We now state the following important Cancellation Theorem.

THEOREM 1. *Let L be a lattice on the regular quadratic space V, and let L' and L'' be two isometric sublattices of L which split L. Then $L'^{\perp} \cong L''^{\perp}$.*

Proof. See [**3**, 92:3].

V. The existence of an extension of the given isometry.

PROPOSITION 2. *Suppose that $q(\eta_i) = \infty$ for all basis vectors of W. Then $W \sim W'$ if $\eta \sim \tau(\eta) = \eta'$ for every $\eta \in W$.*

Proof. There is no loss of generality in assuming that η_1 is primitive and $k_1(\eta_1) = 0$. We consider two cases.

(A) $|\eta_1^2| = 1$,

(B) $|\eta_1^2| < 1$.

https://doi.org/10.4153/CJM-1970-037-x Published online by Cambridge University Press

Case (A). Since $|\eta_1{}^2| = 1$, we can write L as follows: $L = \mathcal{O}\eta_1 \perp L_c$ and $L = \mathcal{O}\eta_1' \perp L_c'$. Write $\eta_j = \alpha_j\eta_1 + \bar{\eta}_j, \bar{\eta}_j \in L_c$ and $\eta_j' = \alpha_j'\eta_1' + \bar{\eta}_j', \bar{\eta}_j' \in L_c'$. Since $\eta_j \cdot \eta_1 = \eta_j' \cdot \eta_1'$, we obtain $\alpha_j = \alpha_j'$. By Theorem 1, we obtain $L_c \cong L_c'$. Since by an easy application of Lemma 9, $\sum c_j\bar{\eta}_j \sim \sum c_j\bar{\eta}_j'$ for all $c_i \in \mathcal{O}$, by induction on the dimension of the lattice, we obtain an isometry $\sigma_1 \in O(L_c, L_c')$ such that $\sigma_1 = \bar{\eta}_j \rightarrow \bar{\eta}_j'$. Define

$$\sigma\begin{cases}\eta_1 \rightarrow \eta_1' & \text{on } \mathcal{O}\eta_1,\\ \bar{\eta}_j \rightarrow \bar{\eta}_j' & \text{on } L_c \text{ via } \sigma_1.\end{cases}$$

Then σ is the required isometry.

Case (B). By Lemma 9, there exist vectors t and t' such that $t \cdot \eta_1 = 1 = t' \cdot \eta_1'$, $t \cdot \eta_j = 0 = t' \cdot \eta_j'$ $(j \neq 1)$, $t^2 = t'^2 = 0$. Write $L = \mathcal{O}\eta_1 + \mathcal{O}t \perp L_c$ and $L = \mathcal{O}\eta_1' + \mathcal{O}t' \perp L_c'$. In this decomposition it is easy to verify that for $j \geqq 2$, $\eta_j = \beta_j t + \bar{\eta}_j, \bar{\eta}_j \in L_c, \eta_j' = \beta_j' t' + \bar{\eta}_j', \bar{\eta}_j' \in L_c'$. Also

$$\beta_j = \beta_j' = \eta_j \cdot \eta_1 = \eta_j' \cdot \eta_1'.$$

Once again $L_c \cong L_c'$ by Theorem 1, and $\sum c_j\bar{\eta}_j \sim \sum c_j\bar{\eta}_j'$. Hence, by induction on the dimension of L, there exists an isometry $\sigma_1 \in O(L_c, L_c')$ such that σ_1: $\bar{\eta}_j \rightarrow \bar{\eta}_j$ $(j = 2, \ldots, r)$. Define

$$\sigma\begin{cases}\eta_1 \rightarrow \eta_1' & \text{on } \mathcal{O}\eta_1 + \mathcal{O}t,\\ t \rightarrow t',\\ \text{equal to } \sigma_1 \text{ on } L_c.\end{cases}$$

Then σ is the required isometry.

PROPOSITION 3. *Suppose that one of the basis vectors, say* η_1, *satisfies the following properties:*

(1) $q(\eta_1)$ *is minimum over all* $q(\eta_i)$ $(1 \leqq i \leqq r)$;

(2) $s(\eta_1) > 1$.

Then $W \sim W'$ *if* $\eta \sim \tau(\eta) = \eta'$ *for every* $\eta \in W$.

Proof. Using Proposition 1, we can choose a decomposition of L so that $\eta_j \in L^{\perp}_{(k_1(\eta_j)-1)}$ for every basis vector η_j. Renumber the basis vectors, if necessary, so that $\eta_1, \ldots, \eta_m$ satisfy the property that $k_1(\eta_i) \leqq q(\eta_1)$ for $1 \leqq i \leqq m$. Then by having chosen the decomposition as mentioned above, we have $\eta_{m+1}, \ldots, \eta_r \in L_{(q(\eta_1))}{}^{\perp}$. Now write $\eta_j = p^{a_1(\eta_j)}\tau_j + \bar{\eta}_j$, where $p^{a_1(\eta_j)}\tau_j \in L_{(q(\eta_1))}$ and $\bar{\eta}_j \in L_{(q(\eta_1))}{}^{\perp}$, for $1 \leqq j \leqq m$. By our choice of the basis vectors, $\tau_1, \ldots, \tau_m$ satisfy Lemma 8. In order to facilitate the notation in the remainder of the proof, we will assume that $\operatorname{ord}(\tau_j{}^2) > \operatorname{ord}(\tau_j)$ and if $\operatorname{ord}(\tau_j) = \operatorname{ord}(\tau_k)$, then $\operatorname{ord}(\tau_j \cdot \tau_k) > \operatorname{ord}(\tau_j)$. (The case in which several τ_j satisfy the property that $\operatorname{ord}(\tau_j{}^2) = \operatorname{ord}(\tau_j)$ gives rise to an almost identical proof, and hence is omitted.)

By an application of Lemma 7, there is a family of $\{t_i\}$ $(1 \leqq i \leqq m)$ of $L_{(q(\eta_1))}$ such that $t_i \cdot \tau_i = p^{\operatorname{ord}(\eta_i)}, t_i \cdot \tau_j = 0$ $(i \neq j)$, $t_i \cdot t_j = 0$ $(1 \leqq i, j \leqq m)$.

By necessity, since $\eta_1 \sim \eta_1'$, we have

$$\tau_1^2 \equiv \tau_1'^2 \pmod{p^{q(\eta_1)}},$$

and since $\eta_1 + \eta_j \sim \eta_1' + \eta_j'$, $\eta_1 - \eta_j \sim \eta_1' - \eta_j'$, we have

$$\tau_1 \cdot \tau_j \equiv \tau_1' \cdot \tau_j' \pmod{p^{q(\eta_1)}} \quad \text{for } 2 \leqq j \leqq m$$

and

$$\tau_1 \cdot \eta_j = 0 = \tau_1' \cdot \eta_j' \quad \text{for } j > m.$$

Decompose $L_{(q(\eta_1))}$ as follows:

$$L_{(q(\eta_1))} = \mathcal{O}\tau_1 + \mathcal{O}t_1 \perp \mathcal{O}\bar{\tau}_2 + \mathcal{O}t_2 \perp \ldots \perp \mathcal{O}\bar{\tau}_m + \mathcal{O}t_m \perp L_c,$$

where $\tau_j = \alpha_{j1}t_1 + \alpha_{j2}t_2 + \ldots + \alpha_{j\,j-1}t_{j-1} + \bar{\tau}_j$, and $\bar{\tau}_j$ is primitive.

By orthogonalization of each hyperbolic plane we can write $L_{(q(\eta_1))}$ as follows:

$$L_{(q(\eta_1))} = \mathcal{O}\lambda_1 + \mathcal{O}\mu_1 \perp \mathcal{O}\lambda_2 + \mathcal{O}\mu_2 \perp \ldots \perp \mathcal{O}\lambda_m + \mathcal{O}\mu_m \perp L_c,$$

where $\lambda_j^2 = -\mu_j^2 = p^{\operatorname{ord}(\tau_j)}$, $\lambda_j \cdot \mu_j = 0$ and $\mathcal{O}\bar{\tau}_j + \mathcal{O}t_j = \mathcal{O}\lambda_j + \mathcal{O}\mu_j$. In this decomposition,

$$\tau_j = \beta_{j1}\lambda_1 + \gamma_{j1}\mu_1 + \ldots + \beta_{jj}\lambda_j + \gamma_{jj}\mu_j \qquad (j = 1, \ldots, m).$$

By our choice of the basis vectors, it is easy to verify, using Lemma 9, that there exists a vector $t \in L_{(q(\eta_1))}{}^{\perp}$ such that

(1) $t \cdot \eta_1 = p^{k_2(\eta_1) + q_2(\eta_1)}$,

(2) $t \cdot \eta_j = 0$ for $j \geqq m + 1$,

(3) $t^2 \equiv 0 \pmod{p^{q(\eta_1)+1}}$.

Now we write $L^{[1]} = L$ in the following form:

$$L^{[1]} = \mathcal{O}(\lambda_1 + \alpha_1 t) + \mathcal{O}\mu_1 + \mathcal{O}(\lambda_2 + \alpha_2 t) + \mathcal{O}\mu_2 + \ldots + \mathcal{O}(\lambda_m + \alpha_m t) + \mathcal{O}\mu_m \perp L_c^{[1]},$$

where $\alpha_1, \ldots, \alpha_m$ lie in $\mathcal{O}$ to be determined. In this new decomposition, we write $\eta_j = \sum p^{a_1(\eta_j)} b_{ji}(\lambda_i + \alpha_i t) + \sum p^{a_1(\eta_j)} \gamma_{ji} \lambda_i + \bar{\eta}_j^{[1]}$, where $\bar{\eta}_j^{[1]} \in L_{(q(\eta_1))}{}^{[1]\perp}$.

Multiplying η_j by $(\lambda_i + \alpha_i t)$ for $1 \leqq i, j \leqq m$ we can solve for b_{ji} and obtain the following.

For $j = i = 1$, we obtain

$$b_{11} = \frac{\beta_{11}\lambda_1^2 + \alpha_1 p^{q(\eta_1)} + p^{q(\eta_1)+1}\delta_{11}}{(\lambda_1 + \alpha_1 t)^2},$$

and for $i \geqq 2$, we obtain

$$b_{1i} = \frac{\alpha_i p^{q(\eta_1)} + \delta_{1i} p^{q(\eta_1)+1}}{(\lambda_i + \alpha_i t)^2},$$

where δ_{1i} is some quadratic polynomial in $\alpha_1, \ldots, \alpha_m$ with integral coefficients.

For $j > 1$, we obtain

$$b_{ji} = \frac{\beta_{ji}\lambda_i^2 + \alpha_i\varphi_{ji}p^{q(\eta_1)} + \delta_{ji}p^{q(\eta_1)+1}}{(\lambda_i + \alpha_i t)^2} \quad \text{for } j \geqq i$$

and

$$b_{ji} = \frac{\alpha_i\varphi_{ji}p^{q(\eta_1)} + \delta_{ji}p^{q(\eta_1)+1}}{(\lambda_i + \alpha_i t)^2} \quad \text{for } j < i,$$

where φ_{ji} lie in the ring and are independent of $\alpha_1, \ldots, \alpha_m$ and δ_{ji} are again quadratic polynomials in $\alpha_1, \ldots, \alpha_m$ with integral coefficients.

It is easy to see that, by choosing $\alpha_1, \ldots, \alpha_m$ appropriately, we will obtain $\eta_j = p^{a_1(\eta_j)}\tau_j^{[1]} + \bar{\eta}_j^{[1]}$ $(j = 1, \ldots, m)$, such that

$$\tau_1^{[1]} \cdot \tau_j^{[1]} \equiv \tau_1' \cdot \tau_j' \pmod{p^{q(\eta_1)+1}} \quad \text{for } 1 \leqq j \leqq m$$

and

$$\tau_1^{[1]} \cdot \eta_j = 0 = \tau_1' \cdot \eta_j' \quad \text{for } j > m.$$

Thus by compactness of the group of integral isometries, there exists a decomposition $L^\infty = L$ such that

$$\tau_1^{\infty 2} = \tau_1'^2,$$
$$\tau_1^\infty \cdot \eta_j = \tau_1' \cdot \eta_j, \qquad 2 \leqq j \leqq m,$$
$$\tau_1^\infty \cdot \eta_j = \tau_1' \cdot \eta_j = 0, \qquad j > m.$$

Write $L^\infty = \mathcal{O}\tau_1^\infty + \mathcal{O}t_1^\infty \perp L_c^\infty$, where $t_1^\infty \cdot \tau_1^\infty = p^{\operatorname{ord}(k_1(\eta_1))}$, $t_1^\infty \cdot \tau_j^\infty = 0$, $t_1^{\infty 2} = 0$, and $L = \mathcal{O}\tau_1' + \mathcal{O}t_1' \perp L_c'$, with t_1' chosen similarly to t_1^∞.

Define

$$\sigma_1: \begin{cases} \tau_1^\infty \to \tau_1', \\ t_1^\infty \to t_1'. \end{cases}$$

Write $\eta_j = \alpha_j t^\infty + \bar{\eta}_j^\infty$, $\bar{\eta}_j^\infty \in L_c^\infty$ $(j > 1)$ and $\eta_j' = \alpha_j' t' + \bar{\eta}_j'$, $\bar{\eta}_j' \in L_c'$. Then since $\sum c_j\bar{\eta}_j^\infty \sim \sum c_j\bar{\eta}_j'$ and $L_c^\infty \cong L_c'$, by induction, there exists an isometry $\sigma_2 \in O(L_c^\infty, L_c')$ such that $\sigma_2: \bar{\eta}_j^\infty \to \bar{\eta}_j'$. Let

$$\sigma = \begin{cases} \sigma_1 & \text{on } \mathcal{O}\tau_1 + \mathcal{O}t_1^\infty, \\ \sigma_2 & \text{on } L_c^\infty. \end{cases}$$

Then σ is the required isometry.

Combining Propositions 2 and 3, we obtain the following result.

MAIN THEOREM. *Let W and W' be two isometric subspaces. Then $W \sim W'$ if and only if $\eta \sim \eta'$ for all $\eta \in W$.*

By the proofs of Propositions 2 and 3 one can see that in order to check for integral equivalence of the subspaces W and W' it is necessary and sufficient to check for complete independence of W and W' restricted to a finite number of sublattices of L and only finitely many vectors of W and W' for critical indices, critical exponents, and congruence relations.

References

1. J. S. Hsia, *Integral equivalence of vectors over depleted modular lattices on dyadic local fields*, Amer. J. Math. *90* (1968), 285–294.
2. D. James and S. Rosenzweig, *Associated vectors in lattices over valuation rings*, Amer. J. Math. *90* (1968), 295–307.
3. O. T. O'Meara, *Introduction to quadratic forms*, Die Grundlehren der mathematischen Wissenschaften, Bd. 117 (Springer-Verlag, Berlin, 1963).
4. A. Trojan, *The integral extension of isometries of quadratic forms over local fields*, Can. J. Math. *18* (1966), 920–942.

Massachusetts Institute of Technology,
Cambridge, Massachusetts;
University of Manitoba,
Winnipeg, Manitoba